KASPERSKY LAB

Kaspersky® Administration Kit version 6.0

Administrator's manual

KASPERSKY® ADMINISTRATION KIT
VERSION 6.0

Administrator’s manual

© Kaspersky Lab

Visit our website: http://www.kaspersky.com/

Revision date: September, 2006

Contents

CHAPTER 1. KASPERSKY ADMINISTRATION KIT

1.1. About Kaspersky Administration Kit

Kaspersky® Administration Kit is designed for centralized performance of key administrative tasks. It gives you complete control over your enterprise antivirus policy, built on the Kaspersky Anti-Virus Business Optimal and Kaspersky Anti-Virus Corporate Suite applications. Kaspersky Administration Kit supports all network configurations that use TCP/IP protocol.

Kaspersky Administration Kit is a tool for corporate network administrators and anti-virus security officers.

The application enables administrators to:

- Deploy and remotely remove Kaspersky Lab applications on and from the network computers. You can create a custom set of Kaspersky Lab applications on a dedicated computer and then install these multiple applications at once on networked computers on any number of networked computers.
- Efficiently manage license keys. With Kaspersky Administration Kit, you can centrally install license keys for all Kaspersky Lab applications, monitor the correspondence between the numbers of licenses and Kaspersky Lab applications installed across your network, and track license expiration dates.
- Remotely manage Kaspersky Lab applications from a single location. With Kaspersky Administration Kit, you can build a multitiered anti-virus protection system managed from one single administrator's workstation. This is particularly important for enterprises with a multiplayer local spread over remote offices. This feature enables the administrators to:

Create *administration groups* of computers with similar functions and applications;

Configure application settings simultaneously by applying *group policies*;

Tailor installations to fit the requirements for individual computers by using *application settings*;

Manage multiple applications by assigning *group and global tasks*;

Schedule tasks for applications installed on computers from different administration groups.

- Automatically update the anti-virus database. You can centrally update the anti-virus database for all applications without having each computer directly connect to Kaspersky Lab update servers. You can schedule updating to run automatically at a specified time to constantly keep your protection current and monitor the update process on client computers.

- Gather reports from all installations. Using the enhanced reporting capabilities of Kaspersky Administration Kit, you can collect statistics about the operation of all installations and create reports based on the most recent statistics. The program allows you to create a cumulative network report for a single Kaspersky Lab application (application-specific reports) or a report about all Kaspersky Lab applications installed on an individual computer (computer-specific report).
- Using mechanism of notifications about specific events in application's operation and notifications sending mechanism. You can specify a set of events which require notification. Such events that may occur during application performance could be, for example, detection of a virus, failure to update, or a new computer appearing on the network.

Kaspersky Administration Kit has three main components:

- Administration Server is a centralized storage of information about Kaspersky Lab applications installed on the local company network and a tool for efficiently managing them.
- Network Agent coordinates the Administration Server and the Kaspersky Lab applications installed on a particular network node (a workstation or a server). This component supports all applications included in Kaspersky Anti-Virus Business Optimal and Kaspersky Anti-Virus Corporate Suite.
- Administration Console, a user interface for Server and Agent Administration services, plugs into the Microsoft Management Console (MMC).

1.2. Hardware and software requirements

Administration Server

- Software requirements:
  - Microsoft Data Access Components (MDAC) version 2.8 and above
  - MSDE 2000 SP 3 or MS SQL Server 2000 SP 3[1] or higher or MySQL version 5.0.22 (default code page UTF-8) or MS SQL 2--5 or higher or MS SQL 2005 Express and higher;

[1] You can install MSDE from the distribution package included in the Kaspersky Administration Kit distribution kit.

  - Microsoft Windows 2000 SP 1 or higher; Microsoft Windows XP Professional SP 1 or higher; Microsoft Windows XP Professional x64 and higher, Microsoft Windows Server 2003 or higher; Microsoft Windows Server 2003x64 or higher Microsoft Windows NT4 SP 6a or higher, MDAC 2.8 or higher.
- Hardware requirements:
  - Intel Pentium III processor, 800 MHz or faster
  - 128 MB RAM
  - 400 MB available space on hard drive

Administration Console

- Software requirements:
  - Microsoft Windows 2000 SP 1 or higher; Microsoft Windows NT4 SP 6a; Microsoft Windows XP Professional SP 1 or higher; Microsoft Windows XP Home Edition SP1 or higher; Microsoft Windows XP Professional x64 or higher. Microsoft Windows Server 2003 or higher; Microsoft Windows Server 2003 x64 and above, Microsoft Windows NT 4 SP 6a or higher;
  - Microsoft Management Console version 1.2 or higher
- Hardware requirements:
  - Intel Pentium II processor, 400 MHz or faster
  - At least 64 MB RAM
  - 10 MB of available hard drive space

Network Agent

- Software requirements:
  - Microsoft Windows 98; Microsoft Windows ME; Microsoft Windows 2000 SP 1 or higher; Microsoft Windows NT4 SP 6a or higher; Microsoft Windows XP Professional x64 or higher, Microsoft Windows XP Professional SP 1 or higher, and Windows Server 2003 or higher; Microsoft Windows Server 2003 x64 or higher
- Hardware requirements:
  - Intel Pentium processor, 233 MHz or faster
  - 32 MB RAM
  - 10 MB available space on hard drive

1.3. Distribution kit

This software product is supplied free-of-charge with any Kaspersky Lab's application included into the package of Kaspersky Anti-Virus Business Optimal and Kaspersky Corporate Suite (retail box version) and also available for download from Kaspersky Lab's corporate website at www.kaspersky.com.

1.4. Help desk for registered users

Kaspersky Lab offers a large service package, enabling its legal users to enjoy all available features of Kaspersky Lab's products .

Once you purchase a license for any Kaspersky Lab's product included into Kaspersky Anti-Virus Business Optimal or Kaspersky Corporate Suite, you become a registered user of Kaspersky Administration Kit. After this you will receive the following services during the term of your license:

- New versions of the anti-virus software application provided free of charge;
- Phone or e-mail consultations on matters related to the installation, configuration, and operation of the anti-virus application by phone or based on requests sent using a web form;

  > When sending a request to the Technical support service, make sure you specify information about the license for Kaspersky Lab's application used in conjunction with Kaspersky Administration Kit.

- Information about new Kaspersky Lab applications and about new computer viruses (for those who subscribe to the Kaspersky Lab newsletter).

> Kaspersky Lab does not provide information related to operation and use of your operating system or various other technologies.

1.5. The purpose of the document

This Guide describes the purpose, general concepts, functions and general operation schemes of Kaspersky Administration Kit application. Step-by-step description of actions is provided in the Kaspersky Administration Kit Reference Book. Functions described in this book are underlined.

In order to review questions that our users often ask Kaspersky Lab's support specialists visit our website and follow the **Services →Knowledge** base link. This section contains information about installation, configuration and functioning of Kaspersky Lab's applications and about removal of most commonly spread viruses and disinfection of infected files.

1.6. Conventions

Various formatting features and icons are used throughout this document depending on the purpose and the meaning of the text. The table below lists the conventions used in the text.

Convention	Meaning
Bold font	Menu titles, commands, window titles, dialog elements, etc.
Note	Additional information, notes.
Attention	Critical information.
To perform an action: 1. Step 1. 2. …	Description of the successive user's steps and possible actions
[key] – modifier name	Command line modifier
`Information messages and command line text`	Text of configuration files, information messages and command line

CHAPTER 2. UNDERSTANDING KASPERSKY ADMINISTRATION KIT

2.1. Logical network

2.1.1. Logical network. Administration Server.

Logical network is a hierarchical structure of *administration groups* consisting of *client computers*. Kaspersky Lab applications installed on client computers are managed through Kaspersky Administration Kit.

Administration Server is a computer on which the Administration Server component is installed.

The Administration server is installed as a service on a computer with the following attributes:

- having name **Kaspersky Administration Server**;
- with the automatic startup at the operating system startup;
- with profile Local system or user's profile depending on the selection made during the component's installation.

The functions of the Administration Server (or, more precisely, of the administration server application installed on this computer) are as follows:

- Store information about the logical network structure (network configuration);
- Store backup copies of the configuration information of the computers in the logical network;
- Store distribution files for Kaspersky Lab applications;
- Remotely install and uninstall applications on the computers;
- Update anti-virus database and program modules;
- Manage *policies* and *tasks* on the computers in the logical network;
- Store information about events occurred on the computers in the logical network;
- Generate reports on application performance across the logical network;

- Distribute license keys across the computers in the logical network, store information about license keys;
- Send alerts from tasks running on the computers in the logical network. You can be notified, for example, about detection of a virus on a client computer.

2.1.2. Hierarchy of the Administration servers

The Administration servers may form hierarchy of type **"main server - slave server"**. Each Administration server may have several slave servers either on one level of hierarchy or using nested hierarchal levels. In this case the structure of the logical network of the main server will include the logical networks of all slave servers. This way, individual independent from each other sections of the computer network can be managed by different Administration servers that, in turn, will be controlled by the main server (details see section 3.5.1 on page 40).

The ability to create a hierarchy of servers may be used:

- to restrict the load on the Administration server (compared with one server installed in the network);
- to decrease the traffic within the network and simplify the interaction with remote offices. There is no necessity to establish connection between the main server and all computers of the network that may be located, for example, in other regions. It is sufficient to install a slave Administration server in each segment of the network, distribute the computers in the logical networks of the slave servers and ensure connection between the slave servers and the main server using fast communication channels;
- to ensure a more distinct division of responsibility between the anti-virus security administrators. All features of centralized control and monitoring of the corporate network anti-virus security status will be preserved.

Each computer included into the logical network structure can be connected only to one Administration server.

The administrator must control the correctness of the computers' connection to the Administration servers using the find computer by network attributes function to search for computers in the logical networks of various servers.

2.1.3. Client computer. Group

Interaction between the Administration server and the computers:

- delivery of information about the current status of the applications;

- sending and receiving of control commands;
- synchronization of the configuration information;
- sending information about events in the applications' operation to the Server;
- functioning of the updating agent;

is ensured by the Network agent. This component must be installed on all computers where the control of the Kaspersky Lab's applications is performed using Kaspersky Administration Kit.

The Network agent is installed on the computer as a service with a set of attributes as follows:

- with name Kaspersky Network Agent;
- with automatic start at the operating system startup;
- with the Local system profile.

A computer, server or workstation on which the Network agent and the monitored Kaspersky Lab's applications are installed will be called the **Server administration client** (or simply *the client computer*).

Depending on the organizational or territorial structure of the company, functions performed and the set of Kaspersky Lab's applications installed, client computers may be organized in *administration groups*. This arrangement may be implemented in order to ensure convenience of managing the computers in the group as a single entity and when arranging computers in the group any combination of the specified principles and other attributed at the administrator's discretion may be used. For example, the top level can be comprised of groups corresponding to the departments. On the next level, within each department, computers will be grouped depending on the function they perform: one group of computers may include all workstations, another all file servers, etc.

A **group** is a set of client computers combined by some attribute in order to control a group computers as a single entity. All client computers in a group share:

- common parameters of the application's operation using *group policies*;
- common application's operation mode - by creating *group tasks* (application functions) with a specified set of parameters (for example, creation and installation of a single *installation package*, updating of the anti-virus database and application modules, on-demand computer scan and real-time protection).

A client computer may be included into one group only.

The administrator may create a hierarchy of servers and groups using any number of nested levels if this simplifies his application administration tasks. Slave Administration servers, groups and client computers may be located on the same hierarchical level.

2.1.4. Administrator's workstations

Corporate network computers running the administration console are referred to as **administrator workstations**. From these workstations, administrators can remotely manage all Kaspersky Anti-Virus components installed across the logical network.

After the installation of the Administration Console an icon for this application will appear in menu **Start/Programs/Kaspersky Administration Kit**.

The administrator workstation is not a logical network object. However, they can be added to the logical network as client computers. The number of administrator workstations is potentially unlimited. Administrator workstations from different Logical Networks can coincide – any logical network can be administered from any administrator workstation available on your local network.

On a logical network, the same computer can act as a client computer, an administration server, and an administrator workstation.

2.1.5. Application administration plug-in

Network Agent Console Plug-in, a special component providing the management interface for specific applications via the Administration Console, is included in all Kaspersky Lab applications managed through Kaspersky Administration Kit. Each application has its own plug-ins installed on the administrator workstation. The plug-ins provide:

- Dialog boxes for creating and editing application policies
- Dialog boxes for creating and editing application settings
- Dialog boxes for configuring task settings
- Information about tasks performed by an application
- Information about events generated by an application
- Information about events and statistics for each client computer sent to the administration console.

2.1.6. Policies, settings, and tasks

A **task** is an action performed by a Kaspersky Lab application. There are several types of tasks, depending on task functions. Each task corresponds to specific application settings.

There is a set of application operating parameters assigned to its task and applied during its execution. The set of parameters of the application, common for all types of tasks, forms the application settings. Application operation parameters specific for each type of tasks form the task settings. The application settings and task settings do not overlap.

For more information about task types, refer to the documentation for Kaspersky Lab applications.

To have an application to perform an action, you should configure application settings, create and configure a corresponding task and run it.

Application settings defined for each individual client computer via a local interface or remotely via an Administration console will be called the **local application settings**.

Centralized configuration of the application operation settings installed on the client computers in the logical network is performed by defining policies.

A Policy – is a set of parameters of an application in a group. **A policy** includes settings for complete configuration of all functions of the application excluding settings specific for individual tasks. An example of such settings are schedule settings.

Therefore a policy includes the following settings:

- common settings for all types of tasks - application settings;
- common settings for all individual tasks of each type – most task settings.

This means that the policy for the anti-virus application (see Figure 1) that includes the real-time protection and on-demand scan tasks, contains all required settings of the application's configuration for execution of both types of tasks, but does not contain, for example, the schedule for execution of these tasks or settings that define the scan scope.

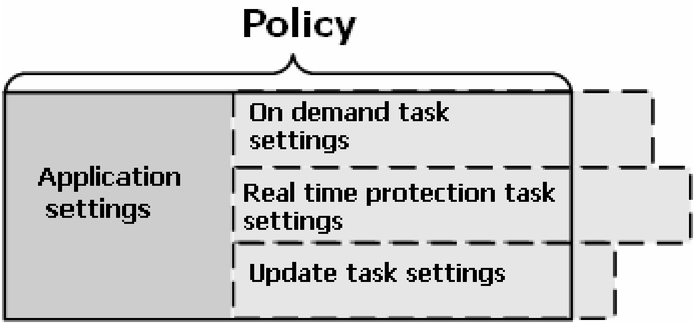


Figure 1. Policy

Each setting in a policy has an attribute, a "lock" that indicates whether changing this setting is allowed in the nested policies in the hierarchal level (for nested groups and slave Administration servers), in the task settings and local application settings. If there is a "lock" attached to this setting, you will not be able to redefine its value (see section 2.1.6 on page 14).

In a group each application will have its own policy defined for it. Several policies with different settings value may be defined for one application. However each application may only have one active policy.

There is a provision that allows the user to activate an inactive policy based on an event, which allows, for instance, to establish stricter anti-virus protection settings during the periods of virus outbreaks.

You can also create policies for mobile users. Such policy will be applied when the computer is disconnected from the corporate logical network.

For different groups the application's operating settings may be different. In each group a separate policy for an application may be created.

Nested groups and slave Administration servers inherit policies of groups of higher level in the hierarchy.

Creation and configuration of tasks across a logical network is centralized. A task assigned to an administration group is a **group task**; a task assigned to an individual client computer is referred to as a **local task**; and that assigned to multiple client computers from different groups on the logical network is a **global task**.

A group task can be assigned to a group even if the application is only installed on some of the client computers in this group. In this case, the group task will be executed only on the computers that have this application installed.

Nested groups and slave Administration servers inherit tasks from their parent groups. A task defined for a group will be shared by all client computers from this group but also by client computers of all nested groups at the lower levels and by slaves Servers on all subsequent levels of the hierarchy.

The tasks assigned locally to a particular client computer will only be executed on this computer. Local tasks will be added to the list of current tasks for this client computer during synchronization of this client with the administration server.

Because all application settings are governed by the policy, you can only redefine settings that have been defined as modifiable by this policy or settings specific to a particular task. For example, for an on-demand scan of a drive, you should specify the disk name, file masks, etc.

You can schedule tasks to start automatically or run them on demand. Task performance results are saved on the administration server. The administrator can be notified of task results or can view detailed reports.

Information about policies, application settings, tasks, and task settings is stored on the server and distributed to the client computers during synchronization. From clients, the administration server receives data about local changes not restricted by the policy, applications running on client computers, their status, and assigned tasks.

2.1.7. Relationship between the policies and the local application settings

Using policies for all computers included into a group, you can set same values for the application's operating settings.

Values of the settings set by a policy can be redefined for individual computers in a group using local application's settings. However, you can set values only for those settings changes to which are not prohibited by the policy: that is their settings should not be "locked".

Which value will be used on the client computer (see Figure 2) is determined by whether the setting is "locked" by the policy.

- if any changes to a setting are prohibited, all client computers will use the same value specified in the policy;
- if changes to a setting are allowed, then each client computer uses a local value of the settings rather than the value specified in the policy. In this case the value of the setting can be changed via the local application settings.

Thus, when a task is being executed on a client computer, the application will use values determined by:

- task settings and local application settings if the policy did not prohibit changes to this setting;
- a group policy, if the policy did not prohibit changes to this setting.

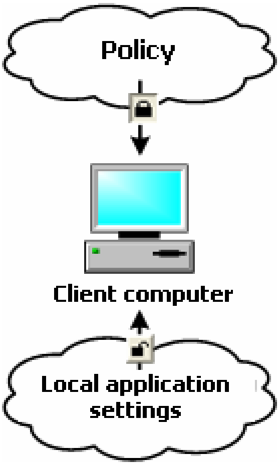


Figure 2. Policy and local application settings

How the local application settings will change after the first time the policy is applied, will be determined in the application policy. If the **Change optional application settings after the policy is first enforced** box (see Figure 12):

- is unchecked, then the *settings that are not allowed to be edited* will be changed after the policy has been enforced; after the policy has been removed the original values of these settings **will not be restored**.

  The values of the *settings that are allowed to be edited* **will not be modified** after the policy has been enforced. Settings **can be modified** using the local application settings. After the policy has been removed, the setting values **will not be changed** (that is, the original values will not be restored).

- is checked, then *the settings that are not allowed to be edited* **will be changed** after the policy has been enforced; after the policy has been removed the original values of these settings **will not be restored**.

  The values of the *settings that are allowed to be edited* **will be changed** after the policy has been enforced. Settings **can be modified** using the local application settings. After the policy has been removed, the setting values **will not be changed** (that is, the original values will not be restored).

2.2. Connecting clients to the Administration server

To enable communication between the clients and the administration server, the client computers must be connected to the server (see section 2.1 on page 11). The Network Agent installed on clients provides this functionality.

The following operations require connection to the server:

- Refreshing the list of applications installed on client computers
- Synchronization of policies, application settings, tasks, and task settings
- Updating the information on applications and tasks running on client computers
- Delivery of events to be processed on the server

In most cases, client computers are connected to the server. This connection is used to automatically exchange data between the clients and the server and to send information about application events to the server.

Automatic synchronization is performed at regular time intervals defined by the Network Agent settings (for example, once every fifteen minutes). The time interval is set by the administrator.

Information about an event is sent to the server immediately after the event occurs.

In the client settings, you can check/uncheck the **Keep connection** checkbox to keep or terminate the client–server connection after the above operations are over. Permanent connection is preferred if connecting to a client is impaired for some reasons (the client is behind a firewall, client ports cannot be opened, the client IP address is unknown, etc.) or you need to constantly monitor the performance of Kaspersky Lab applications.

The administrator can force synchronization to start by clicking the **Force synchronization** command on the shortcut menu of the client computer (see section 2.10.4 on page 29). In this case, the connection is initiated by the server. To enable connection, the UDP port is opened on the client computer. The server sends a connection query to the client's UDP port. In response, the server rights to connect to the client are verified (based on a digital signature), and, if the signature is valid, the connection is established.

A second type of connection is also used to retrieve data from client computers – update the lists of applications and tasks running on the client and refresh application statistics.

2.3. Secure connection to the Administration Server

Data exchange between clients and the Administration Server and connections of the console to the Administration Server are secured by SSL protocol (Secure Socket Layer). SSL protocol is responsible for authentication of communicating parities, encryption of the data being transferred and preventing modification of data during the transfer. Data integrity ensures that the data has not been corrupted or altered in transit. An SSL-enabled connection involves authentication of both sides of a network communication session and encryption of data using the open key method.

2.3.1. Administration Server certificate

Administration Server certificate is used to authenticate the Administration Console when it is connected to the Administration Server and is being established or data is being transferred from client computers.

The Administration Server certificate is created during the installation of the Administration Server. The certificate is stored on the Administration Server, in the **Cert** folder in the installation directory.

The Administration Server certificate can be created only once, during server installation. To restore the certificate, you must reinstall the Administration Server and restore the lost data from the Backup (about backup options, see 6.5 on page 77).

2.3.2. Administration Server authentication (when the Administration Console connects to the server)

When the Administration Console connects to the Administration Server for the first time, it requests the certificate from the server and saves it locally, on the administrator workstation. Upon subsequent connections of the Console to the server with this name, the server will be authenticated using this certificate.

If the server does not pass authentication (i.e., the current certificate differs from that stored on the administrator workstation), the Console informs the user about this and requests the Server for a new certificate. If the connection is successful and another certificate is received, the Administration Console will save the new certificate to the hard disk so that it can be used to authenticate the server in future sessions.

2.3.3. Administration Server authentication when establishing connection with a client

When a client connects to the Administration Server for the first time, it requests the certificate from the server and saves it locally.

> If the Network Agent has been installed on a client locally, the administrator can manually select an Administration Server certificate.

When the client connects to the server next time, the Network Agent will request the certificate from the Administration Server and compare it with the local certificate. If the certificates differ, access to the Administration Server is denied.

If the Administration Server initiates connection, the Network Agent verifies the server's request for a UDP-enabled connection in a similar manner.

2.4. Identification of computers on the logical network

Client computers on the logical network are identified by their **host names**. A host name must be unique among other names connected to this Administration Server.

The name of the client computer is transferred to the Administration Server when a new computer is detected on the Windows network or when the Network Agent installed on a client connects to the Server for the first time after the installation. By default, the host name coincides with the name of this computer on the Windows network (NetBIOS name). If a host with this name already exists, the Server will assign to this host a name ending in a numeral, for example, **Name-1**, **Name-2**, etc. This host name will be used to identify the computer on the logical network.

The Administration Server refers to the client computers by their IP addresses. If a client has an installation of the Network Agent, the IP address of this client is automatically transferred to the Server upon each connection of the client. If the Network Agent is not installed, or this client has not connected to the Administration Server yet (for example, if the Network Agent was locally installed), the Administration Server determines the IP address of this computer by its NetBIOS or DNS name.

2.5. Logical network access rights

Kaspersky Administration Kit provides for the following types of authorization for the access to the application's functionality:

- **Reading:**
    - connecting to the Administration Server;
    - viewing the structure of the logical network (or administration group);
    - viewing the values of the application's policies, tasks, and settings.
- **Execution:** launching and stopping the existing group or global tasks; receiving reports about the applications installed on the client computers.
- **Writing:**
    - creating a logical network, adding groups and client computers to this logical network (or to an administration group);
    - installation of the Network Agent component to the client computer;
    - creating required installation packages for the Kaspersky Lab's anti-virus applications and installing them (along with licenses keys to such applications) on the client computers;
    - updating the version of applications installed on the client computers;
    - creating policies, tasks for groups and individual computers, configuring application settings;
    - centralized administration of applications using services provided by the Administration Server, the Network Agent and the Administration Console components;

- granting to users and groups of users access rights to access the functionality of Kaspersky Administration Kit.

After installation of the Administration server, users included into groups **KLAdmins** and **KLOperators** will be by default granted rights to connect to the Server and to work with the logical network.

Group data will be created during the installation of the Administration server component irrespective of the account selected to launch the Administration server service:

- in the domain that includes the Administration server and on the Administration server computer, if the Administration server is launched under an account of a user included into this domain;
- only on the Administration server computer if this Sever is launched under the system account.

Group **KLAdmins** will be granted all rights: **Reading, Execution, Writing.** Group **KLOperators** will be granted rights **Reading**. The set of rights granted to **KLAdmins** cannot be modified.

Users included into group **KLAdmins** will be called **logical network administrators**, users included into group **KLOperators** – **logical network operators**.

Groups **KLAdmins** and **KLOperators** can be viewed and required changes can be made using standard Windows OS administration tools – **Administration / Local users and groups**.

In addition to users included into group **KLAdmins** the logical network administrator's rights will be granted to:

- domain administrators, computers of which are included into the structure of this logical network;
- local administrators of computers on which the Administration server is installed.

All operations initiated by the logical network administrators will be performed with the rights of the Administration server account. For each Administration server a **KLAdmins** group of its own can be created that will have rights applied within this particular logical network only.

If computers related to one domain create several logical networks, the domain administrator will be the administrator of each logical network formed this way. In this case such logical network will share the same group **KLAdmins** that will be created during the installation of the first Administration server. New members can be added to this group using the operating system's administration tools. Operations initiated by the logical network administrators will be performed with the rights of the corresponding Administration server.

The rights of users in Kaspersky Administration Kit application are determined based on the user Windows authentication in the network.

After the installation of the application, the logical network administrator can (see section 3.2 on page 34):

- change rights, granted to groups **KLOperators**;
- grant rights to access the functionality of Kaspersky Administration Kit application to other groups of users and to individual users registered on the computer on which the Administration Console is installed;

grant various access rights for working with each administration group.

2.6. Deployment of anti-virus protection over logical network computers

There are two common scenarios that show how you can roll out reliable anti-virus protection using Kaspersky Administration Kit:

- You can remotely install applications on client computers across the logical network from a single workstation. The installation and connection to the remote management system proceed automatically, requiring no interaction from the administrator and allowing to install the anti-virus software on any number of client computers.
- You can locally install applications on every networked computer. In this case, all required components and the administrator workstation are manually installed. Connection settings are set during the installation of the Network Agent. This deployment scenario is used only if centralized deployment is impossible.

> Remote installation can be used for installation of any applications selected by the user.
>
> However, bear in mind that Kaspersky Administration Kit supports administration of only Kaspersky Lab's application the distribution package of which includes a specialized component - the application administration plugin.

2.7. Building a centralized anti-virus protection administration system

The first step to building a system of centralized management over an enterprise network through Kaspersky Administration Kit is to design a logical network. At this stage, you should make the following decisions:

Select isolated sections within the network and determine the number of Administration servers that must be installed. It is recommended to ensure interaction between the main and the slave Administration servers using fast communication channels that will allow to considerably decrease the load on the communication channels and increase the system reliability.

Which computers in the corporate network structure will function as the main Administration server, the slave servers administrator workstations, and client computers? Note that all computers on which Kaspersky Lab applications are installed will act as client computers.

What criteria will be used to organize client computers in groups? What will be the group hierarchy?

What deployment scenario will be used: remote or local installation?

In the next stage, the administrator has to build a logical network, i.e., install the following Kaspersky Administration Kit components on networked computers:

Install the Administration Server on computers within the corporate network.

Install the Administration Console on computers from which the administration will be provided.

Make decision regarding assigning of the logical network administrators, determine which other user categories will interact with the system and assign a list of functions to be performed to each category.

Create lists of users and grant to each group access rights required to perform access rights functions assigned to this group.

After this, it is required to create a hierarchy of the Administration servers and for each Server create a logical network structure as follows: create a hierarchy of the administration groups and distribute computers among the corresponding groups.

In the next stage, you should install the Network Agent and selected Kaspersky Lab applications on client computers and install the corresponding Console Plug-ins on the administrator workstation

If you use the remote installation option, the Network agent may be installed together with any application, in this case no separate installation of the Network agent is required.

Finally, you should configure the installed applications by assigning and applying group policies (see section Chapter 4 on page 47) and creating tasks (see section 4.1.2 on page 51).

Using Initial Configuration Wizard, the administrator can easily build an anti-virus protection system for his/her network and briefly configure it (for the detailed description of the wizard, see 3.2 on page 34). Briefly configuring the anti-virus protection system means creating a logical network identical to the domain structure of the Windows network and rolling out the protection system based on Versions 5.0 and 6.0 of Kaspersky Anti-Virus 5.0 for Windows Workstations.

2.8. Maintaining a logical network

After you have created a logical network and installed and configured antivirus applications, it is recommended that you regularly perform the following operations:

- View reports on the results of application performance on client computers.
- Read alerts sent from client computers and the administration server to the administrator’s mailbox.

  > A complete list of notifications sent by the Kaspersky Anti-Virus applications is available in the documentation to these applications.

- If a situation developed on one of the client computers into which the administrator decided to involve, he or she can do it from his own workstation, for example, disinfect infected files on this computer.
- Timely update the anti-virus database on client computers (see Chapter 5 on page 59) and software modules of applications installed on client computers (see Chapter 5 on page 59).
- Keep track of the space available on the server for storing submissions from clients and the availability of free memory on the server to process the submitted data.
- Add new computers that appear on the local network to the logical network and install required anti-virus applications on them in a timely manner.
- Regularly back up the administration system data (see 6.5 on page 77).

2.9. Coordinating joint operation of administrators

The system allows multiple administrators to work simultaneously with the same resources. The latest changes will overwrite previously saved settings. For this reason, joint work of multiple administrators must be coordinated to prevent misunderstanding.

2.10. User interface

From the administrator workstation, you can view, create, modify, and configure the logical network and manage all Kaspersky Lab applications installed on clients. The administration interface is provided by the Administration Console component, which is an administration plug-in integrated into the Microsoft

Management Console (MMC). The Kaspersky Administration Kit interface complies with MMC standards.

In order to ensure local interaction with the client computers, the application includes the ability to establish remote connection with the computer via the Administration Console suing the standard Connect to the remote desktop Microsoft Windows utility.

> In order to use this possibility, you have to allow remote connection to the desktop on client computer.

2.10.1. Launching the application

Kaspersky Administration Kit is launched by selecting item **Kaspersky Administration Kit** in program group **Kaspersky Administration Kit** of the standard menu **Start \ Programs**. This programs group is created only on the administrator's workstations at the time when the Administration Console is installed.

> The logical network Administration server must be launched in order for you to be able to access the functionality of Kaspersky Administration Kit.

2.10.2. Main window

The program main window (see Figure 3) has a menu, a toolbar, a control panel, a view panel, a details panel and a task panel. The menu is used to manage files and dialog boxes and provides access to Help topics. Toolbar buttons provide quick access to most frequently used menu options. The view panel displays the hierarchical **Kaspersky Administration Kit** namespace as a console tree. The details panel shows details of the object selected in the console tree. The details panel provides a quick access to the main operations assigned to the console selected in the tree or in the object’s details panel, by a hyperlink.

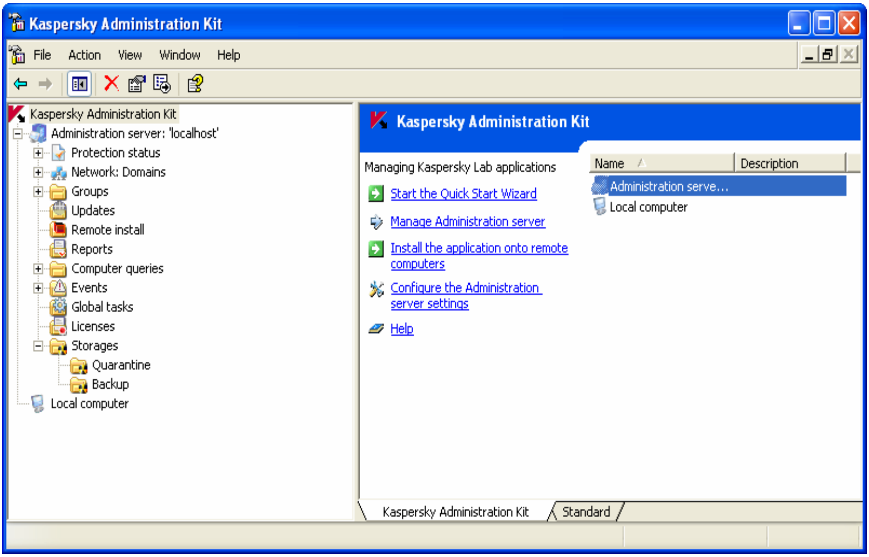

Kaspersky Administration Kit
File Action View Window Help
Kaspersky Administration Kit
Administration server: 'localhost'
Protection status
Network: Domains
Groups
Updates
Remote install
Reports
Computer queries
Events
Global tasks
Licenses
Storages
Quarantine
Backup
Local computer
Kaspersky Administration Kit
Managing Kaspersky Lab applications
Start the Quick Start Wizard
Manage Administration server
Install the application onto remote computers
Configure the Administration server settings
Help
Name
Description
Administration serve…
Local computer
Kaspersky Administration Kit
Standard

Figure 3. Kaspersky Administration Kit main window

2.10.3. Console tree

The console tree displays logical networks created within a corporate network and provides access to the logical network settings and properties of the local computer where the Administration Console is installed.

The **Kaspersky Administration Kit** namespace can have several nodes: the **Kaspersky Administration Server (<Server Name>)** (by the number of Administration Servers) and the **Local computer** object.

Using the **Local Computer** object, you can locally administer Kaspersky Lab applications installed on the administrator workstation.

The **Kaspersky Administration Server (<Server name>)** node is a container that displays the structure and settings of the selected Administration Server. The **Kaspersky Administration Server (<Server name>) KAV Server** node has the following folders:

- Protection status
- Network
- Groups
- Updates
- Remote install
- Computers selections

- Events
- Tasks
- Licenses
- Storages

The **Protection status** folder is used for providing information about the anti-virus protection state both at the client computers and in the computer network as a whole. This folder contains nested report pages that ensure information structure as follows:

- **Network** – information about computers that are not included into the logical network structures and the results of the current of the last polling of the computer network by the Administration server.
- **Administration groups** – the status of the anti-virus protection on the client computers of the logical network.
- **Anti-virus protection** statistics – statistical information about the virus activities on the client computers of the logical network.
- **Updates** – the stat of the anti-virus database used by the applications

The **Network** folder displays the contents of the computer network in which the Administration server is installed. The Administration server creates and updates the information about the network structure and computers included in this network by regularly polling the Windows network and IP subnetworks created in the corporate computer network. The contents of the Network folder will be updated based on this polling.

The **Groups** node is used to store, display, configure, and change the logical network structure, group policies, and group tasks.

Root objects in the **Groups** folder correspond to the highest level of the logical network hierarchy. The **Servers, Policies** and **Tasks** folders are mandatory for each group item. These folders are used to operate Administration servers, policies and tasks of the upper hierarchical level.

The **Updates** folder contains the list of updates received by the Administration server that can be delivered to clients.

The **Remote install** folder contains the list of installation packages that can be used to deploy applications to client computers of the logical network.

The **Reports** folder displays templates of reports on the status of logical network protection.

The **Computers selections** folder is used for search for client computers using specified search criteria, saving the search results and displaying it in individual folders of the console tree.

The **Events** folder displays a list and information about events registered during the operation of the application and about results of the tasks execution.

The **Global tasks** folder has a list of global tasks assigned to a bunch of logical network computers.

The **Licenses** folder shows licenses installed on client computers.

The **Storages** folder is used to manage objects placed by the anti-virus applications into the quarantine folders on the client computers and backup copies of objects placed into the backup storage. However, the objects themselves are not copied to the Administration server.

Information presented in the Administration Console is updated automatically only for nodes.

In order to update the information in the results pane use **F5** key or the **Update** command in the menu, shortcut menu or the **Update** link in the task pane.

2.10.4. Shortcut menu

Every type of object in the **Kaspersky Administration Server** namespace of the console tree has a specific shortcut menu. In addition to the standard MMC commands, these menus contain specific options for treating objects. Additional commands for specific objects are listed in the table below.

Table 1

Object	Command	Action
Kaspersky Administration Kit	**New/Kaspersky Administration Server**	Add an Administration Server to the console tree
<Server name>	**Logon server**	Connect to the administration server
	Disconnect	Disconnect from the Administration Server
	Quick Start Wizard	Launch Quick Start Wizard
	Application Deploy Wizard	Create and run a deployment task
	Find computer	Open a find computer window
	Properties	Display the Administration Server Properties dialog box
	All tasks/Virus attacks detection settings	Configure settings of the virus attack detection on the logical network computers
Network	**Find computer**	Open a find computer window in the **Network** folder
	Application Deploy Wizard	Create and run a deployment task

Object	Command	Action
	View/Domains	Display the computer network structure as the hierarchy of Windows domains and workgroups
	View/Active Directory	Display the computer network structure according to the Active Directory structure
	New/IP sub-network	Create an IP sub-network to display computers
	View/Administration server	Switch to the Administration server node that includes the **Network** folder
	New/IP sub-network	Create an IP sub-network to display computers
	All tasks/computer activity	Configure the Administration server settings response to the absence of computer activities in the network
Groups	**Install application**	Create and run a deployment task for the group
	Update application	Start remote update wizard
	New/Report template	Create a new report template for the selected group
	Find computer	Open a find computer window in the group
	Reset virus counter	Reset virus detection counters on all clients in this group
	Force synchronization	Perform synchronization of data on all computers in the group
	New/Group	Add a new group to the logical network structure
	New/Computer	Adding a new client computer to the group
	All tasks/computer activity	Configure the Administration server settings response to the absence of computer activities in the network
	All tasks / Safety	Configure access rights to the group
	All tasks / Policies	Switch to folder **Policies** for the selected group

Object	Command	Action
	All tasks / Tasks	Switch to folder **Group tasks** for the selected group
	All tasks / Slave servers	Switch to folder **Administration servers** for the selected group
Policies	**New/Policy**	Create a new group policy
Group Tasks	**New/Task**	Create a new group task
	All tasks / import	Import a task from a file
Remote install	**Deployment wizard**	Create an application deployment task
	Applications versions report	Create and view a report about version of Kaspersky Lab's applications installed on computers
	New/Installation package	Create a new installation package
	All tasks / Application deployment task wizard	Create an application deployment task
Reports	**New/Report template**	Create a new report template
Computers selections	**New/New filter**	Create a new filter to search for computers
Events	**View/Filter**	Apply a filter for the event preview table
	All tasks / Import	Import a task from a file
Global tasks	**New/Task**	Create a new global task
Licenses	**Add license key**	Install a new license key
	License keys report	Create and view a report about license keys installed on the client computers
Local computer	**Task**	Open a local computer properties configuration window on the **Tasks** tab

Object	Command	Action
	Applications	Open a local computer properties configuration window on the **Applications** tab

In the details panel, each item selected in the console tree also has a specific shortcut menu with options of how to treat it. The main elements and the corresponding shortcut menu commands are listed in the table below.

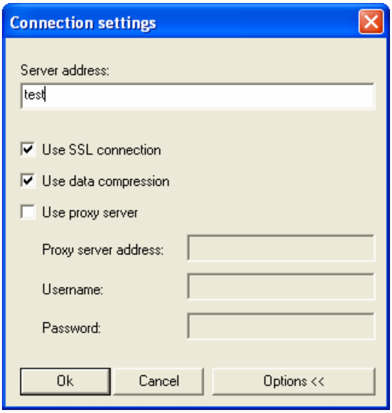
Table 2

Element	Command	Action
Client computer	**Protection**	View information about the client computer anti-virus protection status
	Task	Open a local computer properties configuration window on the **Tasks** tab
	Applications	Open a local computer properties configuration window on the **Applications** tab
	Events	Open a windows for viewing events registered during the operation of the application on the client computer
	Application Deploy Wizard	Create a deployment task for the client computer
	Force synchronization	Synchronize the client computer and the administration server data
	Reset virus counter	Reset virus detection counters on a given client
	Connect to the remote desktop	Open a window for connecting to the remote desktop
Installation Package	**Install**	Create an application deployment task
Report Template	**Generate**	Create and preview the template for the selected report
	Sending reports	Create a task of automation generation and sending reports based on the selected template

CHAPTER 3. USING THE APPLICATION

3.1. Connecting to the administration server

After the startup, the program main application window displays the console tree with the **Kaspersky Administration Kit** namespace at the highest level. To have the program display the logical network structure and settings, you must add the server object to the console tree and connect to the required administration server (see Figure 4). The program receives information about the logical network structure from the administration server and displays it in the console tree.



Connection settings

Server address: test

☑ Use SSL connection

☑ Use data compression

□ Use proxy server

Proxy server address:

Username:

Password:

Figure 4. Establishing connection with the Administration server

Connection attempts will be denied, if the user does not have the connection rights. User rights are verified using the Windows user authentication procedure.

If there are several Administration Servers on your Windows network, you can manage these logical networks from an administration workstation. To select another logical network, connect to the required Administration Server or add several servers to the network tree and connect to one of these servers.

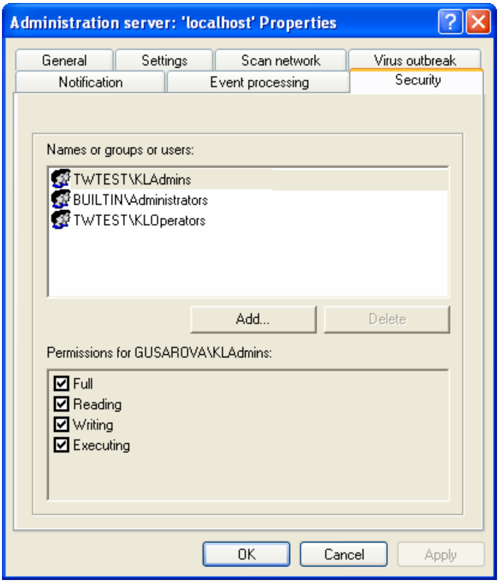
You can only simultaneously manage several Administration Servers and logical networks if you are an operator or administrator of each logical network or have the required rights to each of the networks.

3.2. Granting rights

After the installation of the Administration server, the rights for connecting to the server and working with the logical network will be granted to the users included into KLAdmins and KLOperators groups of the logical network (see section 2.5 on page 21).

You can change the access rights for the KLOperators groups, grant the rights for working with the logical network to other groups of users and to individual users registered at the computer where the Administration Console is installed.

Granting access rights to all objects of the logical networks is performed using the **Security** tab of the Administration server settings configuration window (see Figure 5).



Administration server: 'localhost' Properties

Names or groups or users:

TWTEST\KLAdmins
BUILTIN\Administrators
TWTEST\KLOperators

Permissions for GUSAROVA\KLAdmins:

☑ Full
☑ Reading
☑ Writing
☑ Executing

Figure 5. Granting access rights to the Administration server

There is a provision for an ability to grant separate access rights to each group in the logical network. This setting is configured on the **Security** tab of the group settings windows.

The administrator can track users' actions by events in the operation of the Administration server registered in the events logs. Such events are assigned the **Information message** level of importance and start with word **Audit**.

3.3. Viewing information about the computer network IP subnetworks

Information about the structure of the computer network and about computers within this network is displayed in the **Network** folder of the console tree.

After the installation of Kaspersky Administration Kit the **Network** folder will contain the hierarchy of folders reflecting the structure of domains and workgroups of the corporate Windows network. Each of the folders on the end level contains a list of computers of the respective domain or workgroup not included into the structure of the logical network. Once a computer is included into any group, information about it will be immediately deleted from the folder. Once the computer is excluded from the logical network structure, information about it will again be placed into the corresponding folder of the **Network** node.

The hierarchy of the **Network** node folders may also be reflected based on the Active Directory structures or based on the IP subnetworks created in the network. In order to do it, select **View / Active Directory** or **View / IP-subnetworks** in the shortcut menu of the **Network** node.

If the **Network** node is reflected as IP-subnetworks, its structure may be created by the administrator by creating IP-subnetworks and changing the settings of the existing subnetworks.

When selecting the folders in the console tree, computers included into this folder will be displayed in the results pane as a table in which the following information may be included:

- **Name** – computer's name in the logical network (NetBios name or IP address of the computer).
- **OS type** – indication of the operating system installed on the client computer.

  > Depending on the operation system type an icon will be displayed next to the computer name: – for a server, – for a workstation.

- **Domain** – Windows domain or a workgroup into which the particular computer is included.
- **Agent / Antivirus** – status of the applications installed on the computer. For the Network agent or for the antivirus application that can be managed using Kaspersky Administration Kit a "+" (plus) sign will be displayed if they are installed on the computer. If these applications are not installed, a "-" (minus) sign will be displayed.
- **Visible in the network** – date when the computer was last detected in the network by the Server.

- **Last update** – the date of the last update of the anti-virus database or the applications on the computer.
- **Status** – the current computer status (**OK** / **Warning** / **Critical**) based on the criteria established by the administrator.
- **Information update** – date of the last update of the information about the computer.
- **DNS domain** – a DNS domain to which the computer is related.
- **Domain name** –computer's DNS name.
- **IP address** – computer's IP address.
- **Connection to the server** – time of the last connection of the Network Agent installed on the computer with the Administration server.

The **Network** folder is a reflection of the service group having the same name. Creation and support of the **Network** group in the up-to-date state is performed by the Administration server. The Administration server periodically polls the corporate network to detect any new or disconnection of the existing computers. Based on the obtained information and logical network structure data, the Administration server will update the **Network** group as well as the structure and the contents of the **Network** folder. During the update, computers detected within the network may be automatically included into the structure of the **Network** folder specified by the administrator or into a specified administration group within the structure of the logical network. There is a provision for an ability to disable polling of the computers included into the structure of the **Network** group and into any nested subgroup.

3.4. Quick Start Wizard

Using a wizard built in Kaspersky Administration Kit, you can configure a minimum set of parameters to build a system of centralized management of anti-virus protection. Using this Initial Configuration Wizard, you can configure the following:

- logical network the structure of which, at the administrator's choice, can be:
  - created automatically based on the structure of the domains and workgroups in the Windows network;
  - created manually;
  - imported from a previous version of Kaspersky Administration Kit (versions 4.0 or 4.5) if it was installed in the corporate network.

> If a computer is not registered in the **Network** group at the moment when you are when you are creating a logical network (that is if it is turned off or disconnected from the network), it will not be added to the logical network. You can add this computer later manually.

> Creating a logical network using the Quick Start Wizard does not disturb network integrity: new groups are added; they do not replace the existing groups. A client computer that has been already assigned to an existing group will not be added this time because the **Unassigned** group displays only computers that are not included in the logical network.

- Settings for sending alerts via e-mail or NET SEND about anti-virus protection-related events recorded by the administration server and other Kaspersky Lab's applications.
- The policy and a minimum set of tasks for the highest hierarchical level for versions 5.0 and 6.0 of Kaspersky Anti-Virus for Windows Workstations and global updating tasks for the Administration Server and backup data copying.

> Policies for versions 5.0 and 6.0 of Kaspersky Anti-Virus 5.0 for Windows Workstations is not created if a policy for such applications already exist in the **Groups** folder.
>
> If group tasks for the **Groups** group and the global updating and backup copying tasks with these names have been already created, these tasks will not be formed at this time.

During the first connection to the Administration server after its installation a suggestion to run the Quick Start Wizard will be displayed. In order to run the wizard at a later time, use the **Quick Start Wizard** item from the Administration server's shortcut menu.

3.5. Viewing, creating, and configuring a logical network

The structure of the logical network: the hierarchy the slave administration servers, the list and the structure of the groups are determined at the design stage. The logical network is created in special **Groups** folder (see Figure 6) of the main Kaspersky Administration Kit window by creating the hierarchy of groups and adding to them client computers and slave Administration servers.

Immediately after the installation of Kaspersky Administration Kit the **Groups** folder does not contain any other objects and the **Administration servers, Policies** and **Group tasks** folders are empty. During the creation of the logical network structure by the administrator, client computers and nested groups can be added to the structure of the **Groups** folder.

Groups are displayed as folders; each folder has a structure analogous to that of the **Groups** folder.

- during the creation of each group nested folders **Administration servers, Policies and Group tasks** will be automatically created to store and manage the slave Administration servers, policies and tasks of the particular group;

- when client computers are added to a group, information about the will be displayed as a table in the results pane;
- when a nested group is added a folder with identical structure will be created.

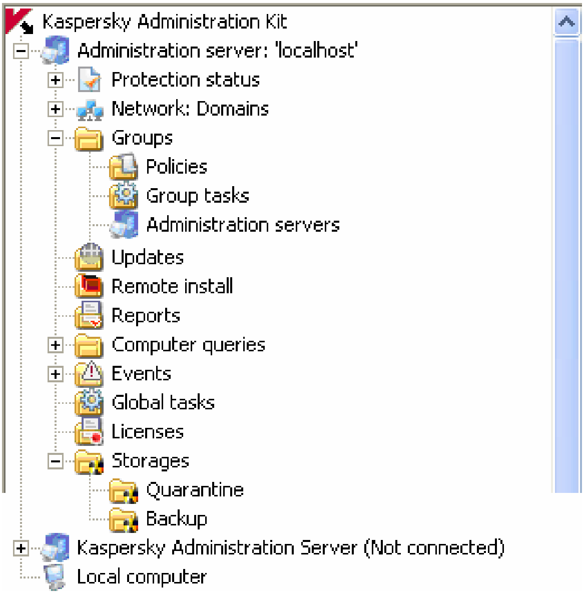


Figure 6. Viewing the logical network objects

When a folder is selected in the console tree, its contest will be reflected in the results pane.

In addition to the information displayed in the table of the **Network** folder the following information about each of the client computers may be displayed:

- **On-demand scan** – date and time of the last full anti-virus scan of the client computer.
- **Viruses detected** – the total number of viruses detected at the client computers since the installation of the anti-virus application (first computer scan) or since the last reset of the value (counter of detected viruses). The value is reset using the **Reset virus counter** from the shortcut menu or the **Action** menu.
- **Real-time protection status** – the current status of the real-time protection of the client computer.

- **Connection IP address** – IP address of the connection between the client computer and the Administration server.

Objects in the Groups folder are managed using the shortcut menu commands (see section 2.10.4 on page 29) and links in the tasks pane.

In order to create a logical network that has a structure identical to the structure of domains and workgroups of the Windows network, you can use the Initial Configuration Wizard (see section 3.2 on page 34).

To create a designed logical network structure manually:

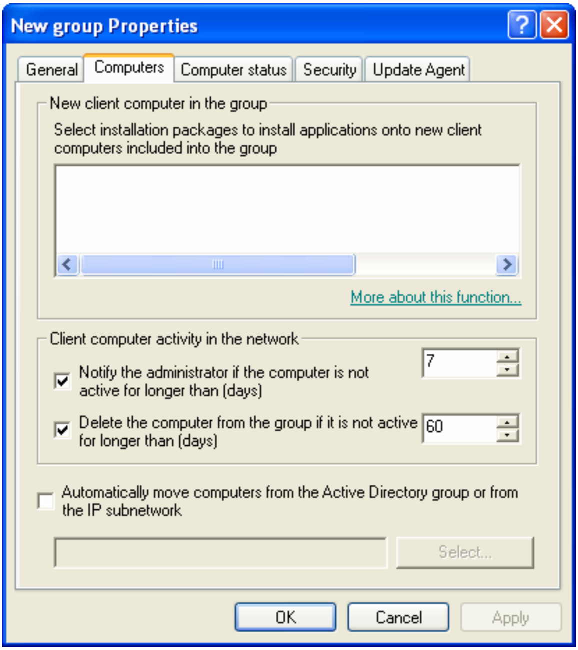
Connect to the administration server required.

Organize a group hierarchy by creating nested groups.

Add client computers to the groups

Add slave Administration servers

The structure of the logical network is reflected in the **Groups** folder. You can obtain information about each object of the logical network: slave servers, groups and client computers. The data provided will contain information when the object was created and when its settings were last modified. You can also review and, if required, modify the settings used by the object (slave server, client computer or all client computer in the group) to interact with the Administration Server.



New client computer in the group

Select installation packages to install applications onto new client computers included into the group

More about this function...

Client computer activity in the network

☑ Notify the administrator if the computer is not active for longer than (days) 7

☑ Delete the computer from the group if it is not active for longer than (days) 60

☐ Automatically move computers from the Active Directory group or from the IP subnetwork

Select...

Figure 7. Viewing the group's properties.
The **Client computers** tab

In order to obtain information about specific client computers, you can utilize the find computer function in the logical network, based on the specified criteria. You can use information about the logical networks of the slave administration servers for the purposes of this search. In order to perform such search and display information about computers in a separate folder of the console tree, use the Create filter function.

If you have any changes in your corporate network configuration, do not forget to make appropriate changes to the logical network. You can:

- Add any number of groups of any nesting level to your logical network (you can add slave Administration servers and nested groups that form next hierarchy level to a group).

You can also define what Kaspersky Lab applications will be automatically installed on all client computers of this group.

> To enable automatic installation of Kaspersky Lab applications on new networked computers running Microsoft Windows 98/ME, the Network Agent must be installed on them.

- Add client computers to groups.
- Change the hierarchical order of objects on the logical network by moving individual client computers and entire groups to other groups.
- Add slave Administration servers to the logical network structure in order to reduce the load on the master Server, decrease the internal traffic and increase the remote administration system reliability.
- Move client computers from one logical network into another.

3.5.1. Groups

In order to add a new group, use command **New / Group** from the shortcut menu of the group to which the nested group is being added. As the result, in the console tree, in the **Groups** node (see Figure 6) included into the folder you specified a new folder with the indicated name will appear. Nested folders **Policies, Group tasks** and **Administration servers** will be automatically created in this folder. They will be filled during the stage of defining group policies, creation of group tasks and slave Servers.

Client computers and nested groups that form next hierarchal level can be included into this group.

You can also define which Kaspersky Lab's applications will be automatically installed on all client computers added to the group.

> For automatic installation of Kaspersky Lab's applications onto new computers running OS Microsoft Windows 98/ME, Network Agent must have been installed on these computers.

In the future you can change the name of the group, move it to another group or delete it.

A group is moved along with all nested groups, slave Administration servers, client computers, group policies and tasks. All settings corresponding to its new status in the hierarchy of the logical network objects will be applied to this group.

A group can be moved using standard shortcut menu commands **Cut / Paste** or similar items in the **Action** menu and also using a mouse.

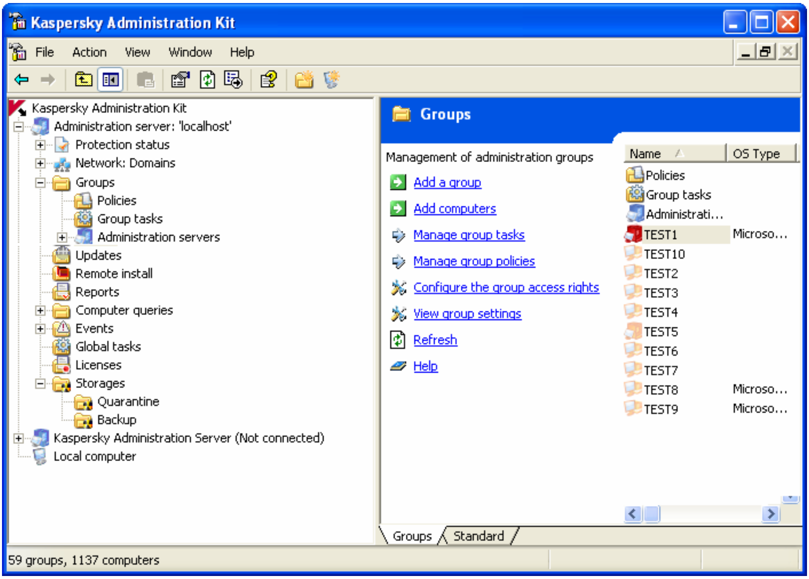
When moving a group, note that the rule requiring unique name of each group within one level of hierarchy must be observed. In order to resolve a naming conflict, rename the group before you move it. If you do not observe this rule suffix **_1, _2,** etc. will be automatically added to the name.

> You cannot rename the **Groups** folder because it is an in-built element of the Administration Console.

A group can be deleted from the logical network if it does not contain slave Administration servers, nested groups and client computers and it has no tasks and policies created for it. You can delete a selected group using the **Delete** command from the shortcut menu or the analogous item in the **Actions** menu.

3.5.2. Client computers

In order to add client computers to a group, use command **New / Computer** from the shortcut menu of the group to which you are adding the computers. This will launch the corresponding wizard. Once the wizard completes successfully, the computers will be included into the group and will be displayed in the results pane under names determined by the Administration server (see Figure 8).

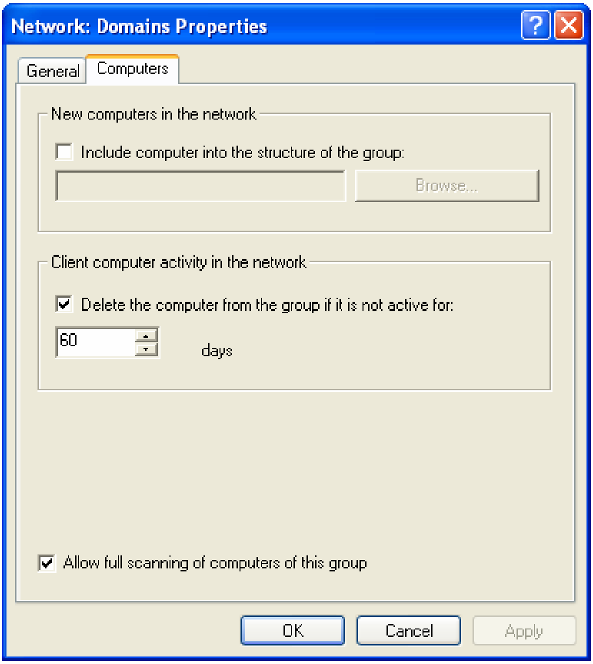


Name	OS Type
Policies	
Group tasks	
Administrati...	
TEST1	Microso...
TEST10	
TEST2	
TEST3	
TEST4	
TEST5	
TEST6	
TEST7	
TEST8	Microso...
TEST9	Microso...

Figure 8. Client computers in a group

Adding client computers to the logical networks can be configured in such a way that the Administration server will be automatically including all computers detected into the specified administration group. For this the corresponding settings must be configured in the **Network** group properties (see Figure 9).

A computer can also be added in the main application window of Kaspersky Administration Kit by dragging the computer from the **Network** folder to the logical network folder with the mouse.



New computers in the network

□ Include computer into the structure of the group:

Client computer activity in the network

☑ Delete the computer from the group if it is not active for:

60 days

☑ Allow full scanning of computers of this group

Figure 9. Configuring automatic moving of new computers to a group

You can move client computers from one group to another by excluding them from the logical network using standard shortcut commands **Cut / Paste** and **Delete** or analogous items from the **Action** menu. Computers deleted from the logical network will be moved to the **Network** group. The moving operation can also be performed using the mouse.

Client computers can be moved from one logical network to another. For example, when adding a slave Administration server, you can move client computers from the Master Server logical network to a slave Server logical network. In order to do it, the client computers must be connected to the new Administration server.

Connecting the client computer to another Administration server shall be performed by creating and launching the **Change Administration server** task. It is possible to move either individual computers by creating a global task or all client computers from a specific administration group using a group task. As a result of execution of the **Change Server** task, the client computers for which this task was created and successfully completed, will be disconnected from the old Administration server and will then appear in the **Network** group of the new Server. Client computers can be deleted from the administration groups of the old logical network and added to a new logical network manually using the Administration Console.

You can connect a client computer to a different Administration Server locally from the client computer.

This operation is performed using utility ***klmover.exe*** included into the Network Agent distribution package. After the installation of the Network Agent this utility will be located in the root installation folder of the component.

3.5.3. Slave Administration servers

Using the server hierarchy the following operation can be performed for all slave Administration servers and client computers connected to it from the main Server:

- *application policies* can be created and distributed;
- *group tasks* (including deployment tasks) can be created and distributed;
- *updates* and *installation packages* received by the main Server can be distributed;
- *reports* with consolidated information on all slave Administration servers can be created.

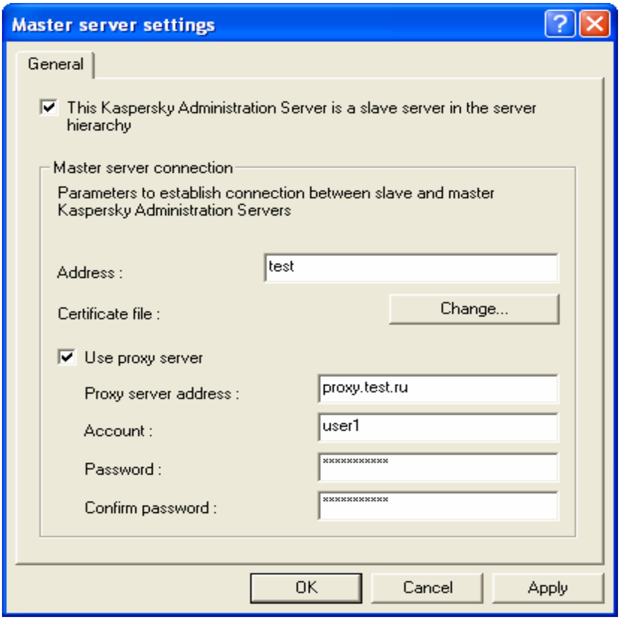
The policies and tasks received from a master Administration Server are not available for modification on a slave server.

In order to add a slave Server use the **New / Administration server** item for the Administration server object in the group as required. This will start the slave server adding wizard. This wizard will perform the following:

- adding a slave Administration server;
- connecting the Administration Console to the slave Server;
- configuring setting of connection to the main Server.
- adding information about the slave Server tot he database of the main Administration server.

You can skip the connection and configuration stages and perform the manually at a later time. In order to do it connect to the Server that will be used as the slave Server via the Administration Console and indicate settings for its connection to the main Server (see Figure 10).

After the slave Administration server has been successfully added, the Server's icon and the name will be displayed in the corresponding group in the **Administration servers** folder.



☑ This Kaspersky Administration Server is a slave server in the server hierarchy

Master server connection

Parameters to establish connection between slave and master Kaspersky Administration Servers

Address : test

Certificate file : Change...

☑ Use proxy server

Proxy server address : proxy.test.ru

Account : user1

Password : ************

Confirm password : ************

Figure 10. Configuring settings for connection
to the main Administration server

You can manage the logical network of the slave Administration server via the **Administration servers** node of the main Server's logical network or directly by adding the Server to the console tree as a new Administration server.

- The slave Server is a full-fledged Administration server and performs all functions of the Administration server within its logical network.

Additionally a slave Administration server inherits from the main Server all group tasks and policies of the group into which it is included. Inherited policies and tasks area reflected on the slave Server as follows:

- Icon 📜 will be displayed next to the policy name received from the main Administration server. (The regular policy icon is 📜).
- The values of the settings of the inherited policy will not be accessible for changes on the slave Server.
- Settings that are not allowed to be modified in the inherited policy are not accessible or changes (icon 🔒) in all application policies on the slave Server and use values specified in the inherited policy.
- Values of the settings that are allowed to be modified in the inherited policy can be changed in policies of the slave Server (icon 🔓). If the setting

was not "locked" in the slave Server policy, it can be changed in the application or task settings (see section 2.1.7 on page 17).

- Icon ⚙ will be displayed next to the group task name received from the main Administration server. (The regular task icon is ⚙).

Global deployment tasks cannot be transferred to the slave Servers. The transfer of group tasks is configured in the task properties.

Updating of the slave Administration Server client computers can be configured in such a way that after the updates have been received by the main Server a task for receiving updates by the slave Server will be automatically launched and after this task has been successfully completed tasks for updating applications on the slave Administration Server's client computers will be launched (see section 5.3 on page 65).

CHAPTER 4. REMOTE POLICY MANAGEMENT

Kaspersky Administration Kit supports administration of only those Kaspersky Lab's applications that have a specialized component - application administration plugin included into their distribution package.

4.1. Configuring the application settings

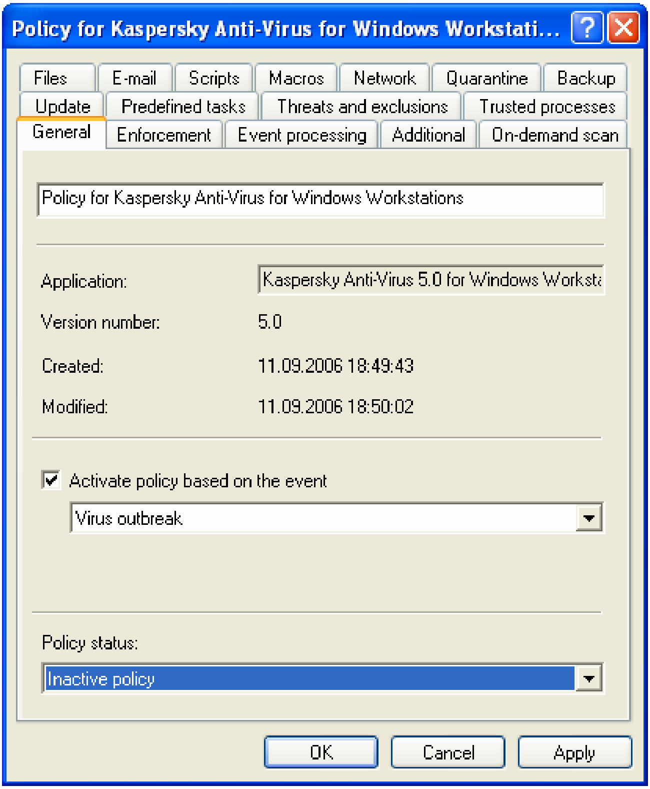
4.1.1. Managing policies

You can only create a policy for an application if the plug-in for this application is installed on the administrator workstation.

To create a policy use the **New / Policy** command from the shortcut menu of the **Policy** folder. At this stage of the policy creation, you configure a minimum set of parameters required for operation of the application. All other settings are set by default and correspond to default values applied during the local installation of the application.

A detailed description of the policy settings for Kaspersky Lab's applications is provided in the Manuals for these applications.

Later you can modify the values of the settings, prohibit changes to them in the policies of nested groups and in the application's settings (see Figure 11).



Policy for Kaspersky Anti-Virus for Windows Workstations

Application: Kaspersky Anti-Virus 5.0 for Windows Workst

Version number: 5.0

Created: 11.09.2006 18:49:43

Modified: 11.09.2006 18:50:02

☑ Activate policy based on the event

Virus outbreak

Policy status:

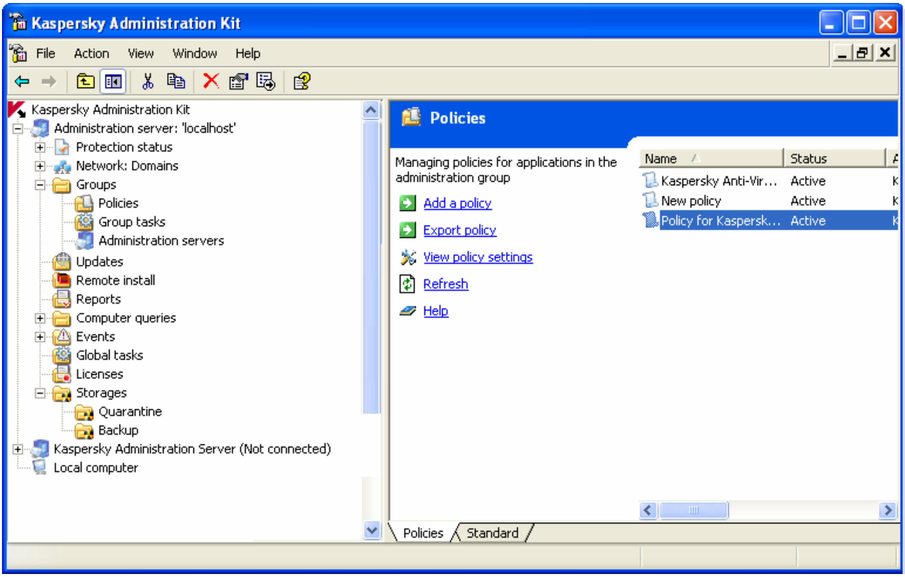
Inactive policy

Figure 11. Editing policies

Settings, governed by the policy, modification of which is prohibited, will be marked by icon. In order to prohibit changes, left-click it. The icon will be changed to. These settings will then become inaccessible for changes using the application's settings, tasks settings and policies of the nested groups and slave Administration servers.

Local settings have higher priority as compared to the policy settings (see section 2.1.7 on page 17). If you wish to use a value specified in the policy for a particular settings, you must lock such setting.

After a new policy is created, it is added to the **Policies** folder (see Figure 12) of the corresponding group and will be applied to all nested groups and slave Administration server included into such group as the inherited policy.



Managing policies for applications in the administration group

Name	Status	A
Kaspersky Anti-Vir...	Active	K
New policy	Active	K
Policy for Kaspersk...	Active	K

Figure 12. The **Policies** folder

You can delete, copy, export or import crated policies from one group to another using the shortcut menu commands of the policy selected in the results pane.

Several group policies may be created for each application, however there can be only one active policy. Such policy must have the **Active policy** parameter selected in its settings.

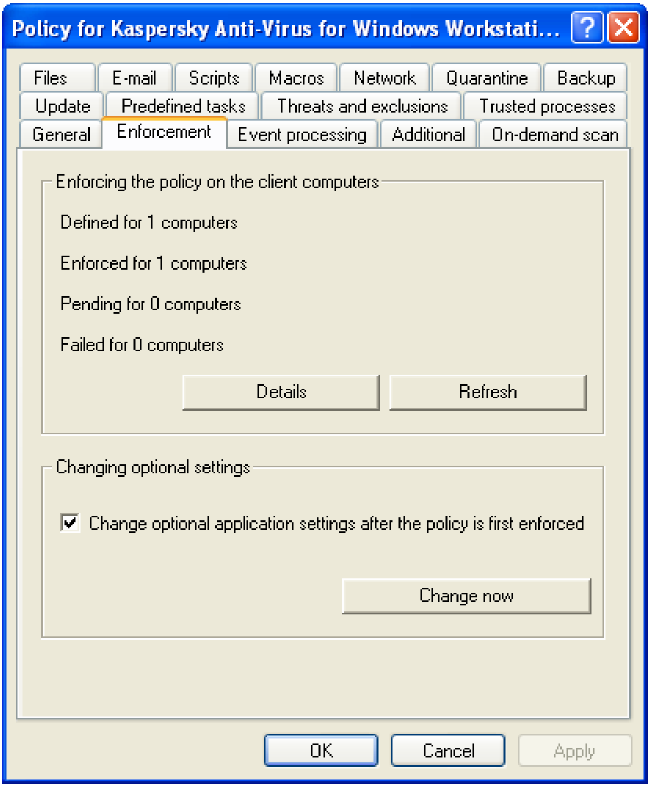
The policy can be activated automatically, triggered by a certain event. However, you can return to the previous policy only manually.

You can also create a policy for mobile users that will be enforced immediately after the computer is disconnected from the corporate logical setting.

The results of the policy deployment can be viewed via the Management Console in the Administration Server policy properties window (see Figure 13).

The way the values of the local application's settings change on each client computer depends on the status of the **Change optional application settings after the policy is first enforced** box (see section 2.1.7 on page 17).

Additionally, you can match the settings to the selection you have made manually irrespective of whether the policy has been enforced. In order to do it press the **Change now** button (see Figure 13).



Enforcing the policy on the client computers

Defined for 1 computers

Enforced for 1 computers

Pending for 0 computers

Failed for 0 computers

Changing optional settings

☑ Change optional application settings after the policy is first enforced

Figure 13. Policy enforcement settings configuration

The policy will be applied in the following way. If resident tasks (real-time protection) were running on a client, they will seamlessly switch to the new settings' values. If there are periodic tasks currently running on a client (on-demand scans, database updates), they will continue working with old values. The new settings' values will be applied upon the next startup of these tasks. You can view the application settings, after the new policy has been applied, via the Management console in the properties window of the specific client computer.

In case of a hierarchical structure, slave administration servers retrieve policies from the master Server and then apply these policies on client computers. Policy settings can be changed only on the master Administration Server. After this, the slave servers correspondingly modify the policies and deploy them through client computers.

The results of policy deployment on slave administration servers are displayed in the policy properties window on the master Administration Server.

You can similarly view the results of the policy deployment on the client computers in the policy properties window of the slave administration server after you connect to it.

A detailed description of the policy settings for Kaspersky Lab's applications is provided in the applications' Guides. Policy configuration for the Network Agent and the Administration server is described in the Reference Book for Kaspersky Administration Kit.

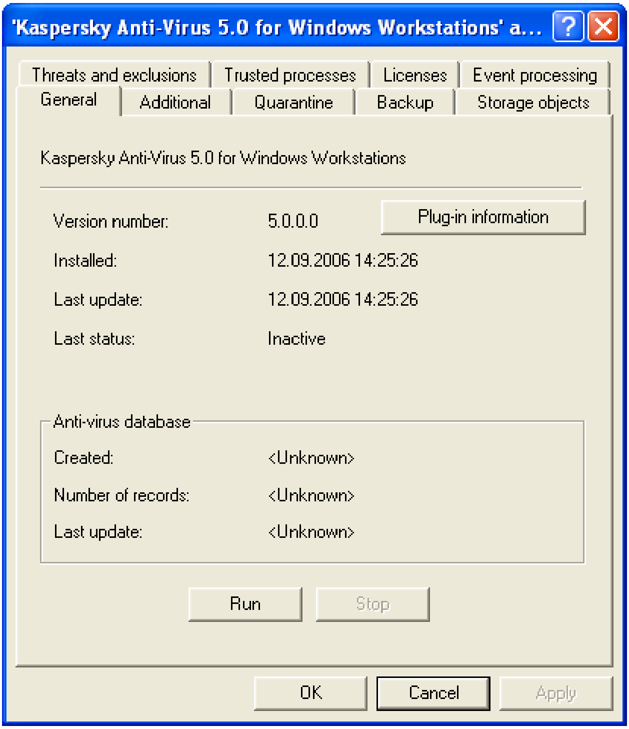
4.1.2. Local application settings

Kaspersky Administration Kit system allows remote administration of the settings of the local applications installed on the client computers using the Administration Console (see Figure 14). Using the application's settings, you can set up individual values of the application's operation settings for each client computer in the group. You can change values only for those settings modification of which is not prohibited by the group policy for a particular application, that is the setting is not "locked" in the policy.

Local settings configuration is performed for each client computer separately in the **"<Application name>" Application Settings.** This window is called from the **Application** tab of the **Properties** window**: <Computer name>.**

> Each Kaspersky Lab's application has its own set of local settings. A detailed description of these settings see Manual of the particular application.

A detailed description of the Network Agent and Administration server settings is provided in the Kaspersky Administration Kit Reference Guide.



Kaspersky Anti-Virus 5.0 for Windows Workstations

Version number: 5.0.0.0

Installed: 12.09.2006 14:25:26

Last update: 12.09.2006 14:25:26

Last status: Inactive

Anti-virus database

Created: <Unknown>

Number of records: <Unknown>

Last update: <Unknown>

Figure 14. Local application settings configuration window

4.2. Managing the application

Managing of the operation of applications installed on the client computers in the logical network is performed by creating and launching tasks implementing all major functionality: installation of applications and license keys, scanning of files, updating of anti-virus database and application modules, etc.

Kaspersky Administration Kit supports all types of tasks provided for the local application management. Additionally, there is a provision for a remote launching and stopping applications using corresponding Network Agent administration tasks. Detailed description of tasks types for each Kaspersky Lab's application is provided in the Guide for the particular application.

Via the Administration Console remote launching and stopping of the application is performed using corresponding tasks.

Creating tasks for an application is possible only if an administration plugin for this application is installed on the administrator's workstation.

In order to ensure network protection the administrator can create any number of various tasks (except tasks that can be created only once) for all applications that are managed using Kaspersky Administration Kit.

For example, in order to scan client computers that are workstations, for malware, you have to create an On-demand scan task for Kaspersky Anti-Virus for Windows Workstations.

Application management functions and general service operations perform tasks of the Kaspersky Administration Kit, Administration server and Network Agent components. The following type of tasks are defined for this component:

- **Change of the Administration server**.
- **Launching / stopping the application**.
- **Application deployment**.
- **Application remote uninstallation**.
- **Receiving updates by the Administration server**.
- **Creating a backup copy of the Administration server**.
- **Sending reports**.
- **Distribution of the installation package**.

Tasks of these types have several distinctive features as far as creation and launching are concerned. A detailed description of managing these tasks is provided in the Kaspersky Administration Kit Reference Book.

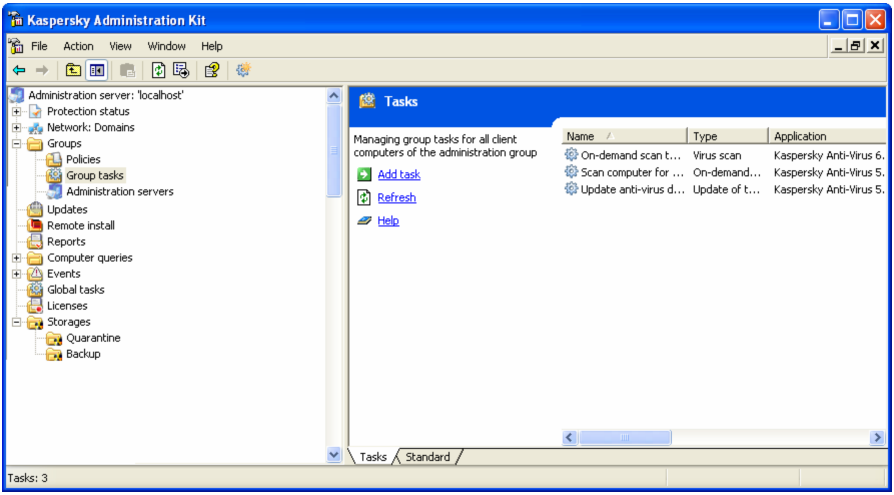
You can create group, global, and local tasks for all types of tasks.

For the **deployment** both group and global tasks can be created. For **receiving updates**, **creating a backup copy** and **sending reports** tasks only global tasks can be created.

> **Receiving updates** and **Creating a backup copy of the Administration server** tasks can only be created in single entities and can be executed for one computer only - the Administration server.

In order to create a task use the **New / Task** command from the shortcut menu for the **Group tasks** folder or the **Global tasks** folder.

Created group tasks will be located in the nested folders **Group tasks** of the corresponding groups (see Figure 15). Global tasks will be located in a special container in the console tree called **Global tasks**. You can review the list of local tasks of the client computer in the client computer properties window.



Managing group tasks for all client computers of the administration group

Name	Type	Application
On-demand scan t...	Virus scan	Kaspersky Anti-Virus 6.
Scan computer for ...	On-demand...	Kaspersky Anti-Virus 5.
Update anti-virus d...	Update of t...	Kaspersky Anti-Virus 5.

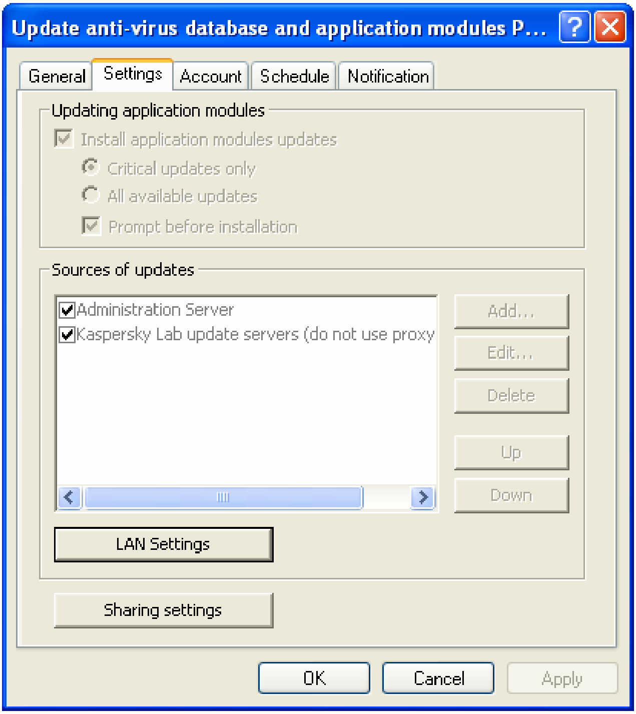
Figure 15. Group tasks

Exchange of information about tasks between the local application and Kaspersky Administration Kit information database takes place at the moment when the Network Agent connects to the Server: The information about locally created tasks will be transferred to the Administration server database.

You can modify the task settings, monitor their execution, copy, export or import tasks from one group into another or delete them using the shortcut menu commands.

During execution of tasks on each client computer, the application operation settings will be installed in accordance with the group policy, task settings and settings of the particular application installed on the client computer (details see section 2.1.7 on page 17).

Most of the settings are defined by the policy of the application that performs this task. For example, actions with infected objects upon their detection, resource to be used for updating the anti-virus database, etc. If these settings are locked against changes in the policy, they cannot be changed in the task settings (see Figure 16).



Update anti-virus database and application modules P...

Updating application modules

☑ Install application modules updates

● Critical updates only

○ All available updates

☑ Prompt before installation

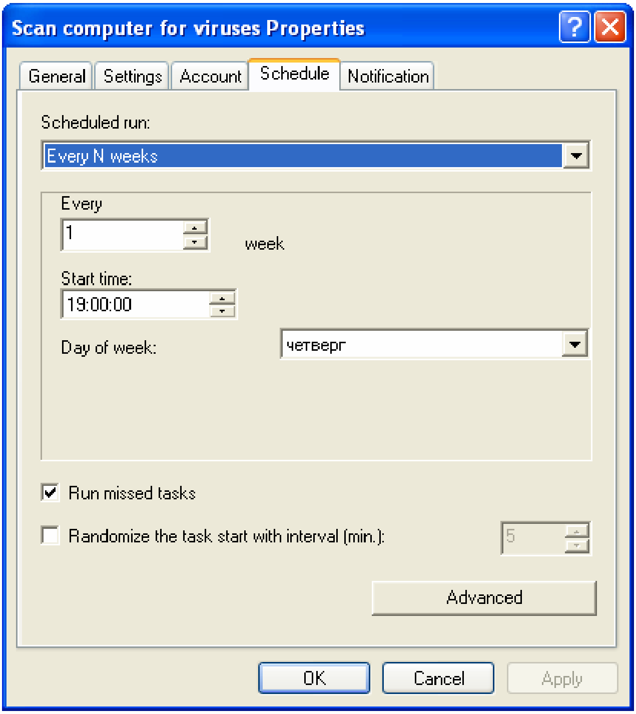
Sources of updates

☑ Administration Server

☑ Kaspersky Lab update servers (do not use proxy

Figure 16. Task settings locked in the policy

However, a part of the settings is specific to a particular task: schedule for launching a task, account under which the task is launched, scan scope for on-demand scan tasks, etc. Values of these settings are set for each task in its settings and can be changed after the task is created (see Figure 17).



Scheduled run: Every N weeks

Every 1 week

Start time: 19:00:00

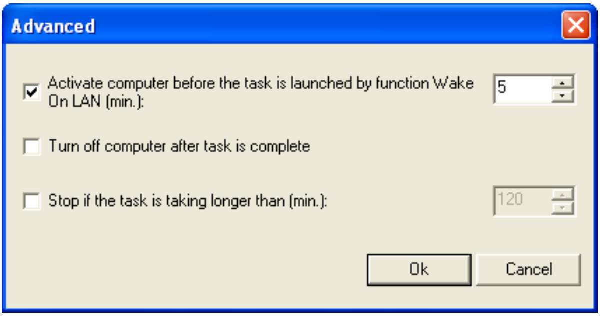
Day of week: четверг

☑ Run missed tasks

□ Randomize the task start with interval (min.): 5

Figure 17. Task launch schedule

Tasks will be launched in accordance with the schedule On computers that are going to be turned off during the scheduled launch time, the operating system can be automatically loaded using the Wake On Lan function. In order to use this function, you must check the corresponding box (see Figure 18) on the **Schedule** tab (see Figure 17) that opens by pressing the **Advanced** button.



☑ Activate computer before the task is launched by function Wake On LAN (min.): 5

□ Turn off computer after task is complete

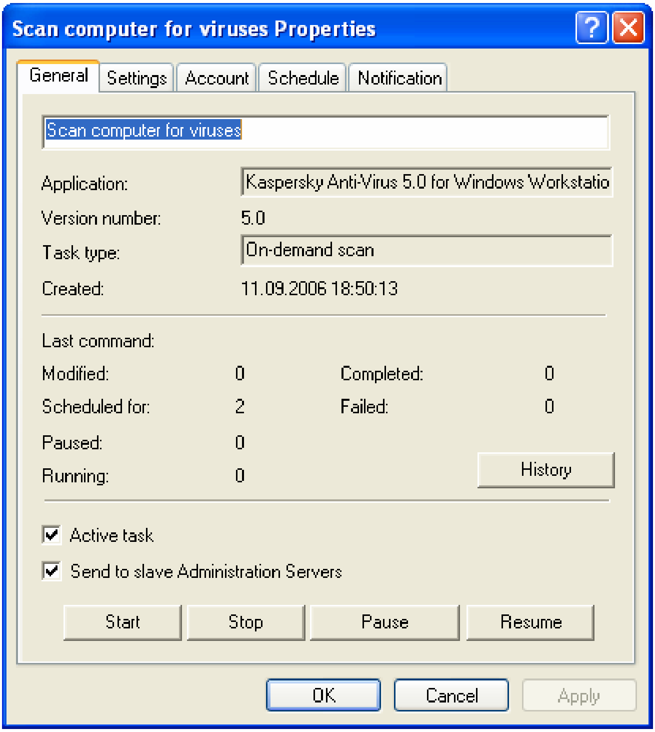
□ Stop if the task is taking longer than (min.): 120

Figure 18. Enabling automatic operating system loading

You also can enable automatic computer turn off after the scheduled task has been completed.

The task execution time can be restricted; in this case the task will be stopped once the time period specified in the time settings has been elapsed. There is a possibility to disable scheduled task launch. In this case the task will not be deleted, but it will not be launched either.

Additionally, you can start a task, interrupt it, pause or resume a task manually using the shortcut menu commands or from the task settings viewing window (see Figure 19).



Scan computer for viruses

Application: Kaspersky Anti-Virus 5.0 for Windows Workstatio

Version number: 5.0

Task type: On-demand scan

Created: 11.09.2006 18:50:13

Last command:

Modified: 0 Completed: 0

Scheduled for: 2 Failed: 0

Paused: 0

Running: 0

☑ Active task

☑ Send to slave Administration Servers

Figure 19. Managing task execution

Tasks on the client computer are executed only if the corresponding application is running. Once you close the application, all running tasks will be terminated.

You can monitor task execution and view results of its execution in the task settings window (seeFigure 19).

Results of tasks execution are registered and saved in accordance with the settings in the Windows event logs and Kaspersky Administration Kit events logs either in a centralized location on the Administration server or on each client computer locally. The administrator and other user can be notified about the results of the tasks execution; the form and the method of notification will also be determined by the task settings.

You can view the results of the task execution registered in the Kaspersky Administration Kit via the **Events** node of the console tree. You can review results of tasks execution for each client computer in this computer's properties window.

The information about the results of the task execution stored locally on a client computer can be viewed via a local Administration Console installed on this computer.

With the hierarchal structure of the Administration servers, if the corresponding parameter is included into the task settings (see Figure 19), the slave Servers will receive group tasks from the main Administration server and then distribute them to the client computers. The group task's settings can be modified on the main Administration server. After this the slave Administration servers will accordingly modify their group tasks and distribute them to the connected client computers.

Results of the distribution of a group task to the slave Administration servers will be reflected in the **Task execution results** window of the Administration server group task properties window.

Similarly, you can review the results of the group task distribution to the client computers in the slave Administration server group task properties window after you have connected to the slave Administration server.

CHAPTER 5. UPDATING THE ANTI-VIRUS DATABASE AND PROGRAM MODULES

Regularly updating the anti-virus database, installing updated program modules (patches), and upgrading program versions are critical factors for keeping your network constantly protected from any threats.

The Kaspersky Lab web-based anti-virus database is updated on an hourly basis. We strongly recommend that you update your anti-virus database with the same frequency and install all program patches in a timely fashion.

To update anti-virus database and program modules of the applications managed through Kaspersky Administration Kit, you have to create a global task to Kaspersky Administration Kit to retrieve updates. Kaspersky Administration Kit will download the updated database and modules from an update source, according to the global task settings. The downloaded updates will be stored on the Administration server in public folder Updates from where they can be automatically distributed across the client computers and slave Administration servers immediately after the updating has been completed. The public access folder is created during the installation of the Administration server. By default it is the **Share** folder located in the Administration server component installation **(<Drive>:\Program Files\Kaspersky Lab\Kaspersky Administration Kit)**.

The updates are distributed on the client computers using the application updating tasks. Updating of the slave Servers is performed using the task of receiving updates by the Administration server. These tasks can be launched automatically immediately after receiving the updates by the master Server irrespective of the schedule setup in the task settings.

5.1. Receiving updates by the Administration server

The Receiving updates by the Administration server task is a global task and only one instance of this task can be created. This task is created and run only for one computer - the computer on which the Administration server is installed.

If you used the Quick Start Wizard, the task of receiving the Administration server has been already created and located in the **Global tasks** node of the console tree.

In order to create the task for receiving updates by the Administration server, launch the task creation wizard for the **Global tasks** node. As the application for which the task is created select **Kaspersky Administration Kit**, as the type of the task - **Receiving updates by the Administration server** (see Figure 20).

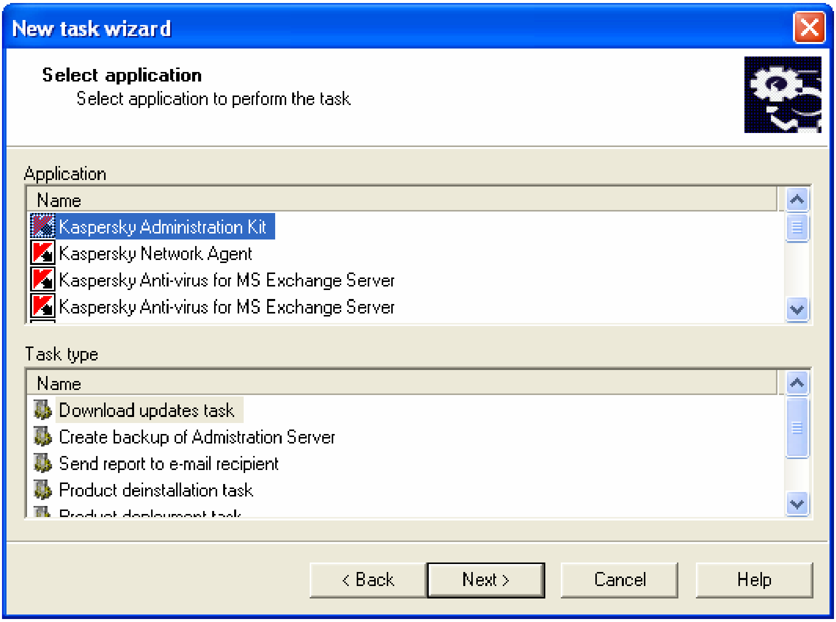
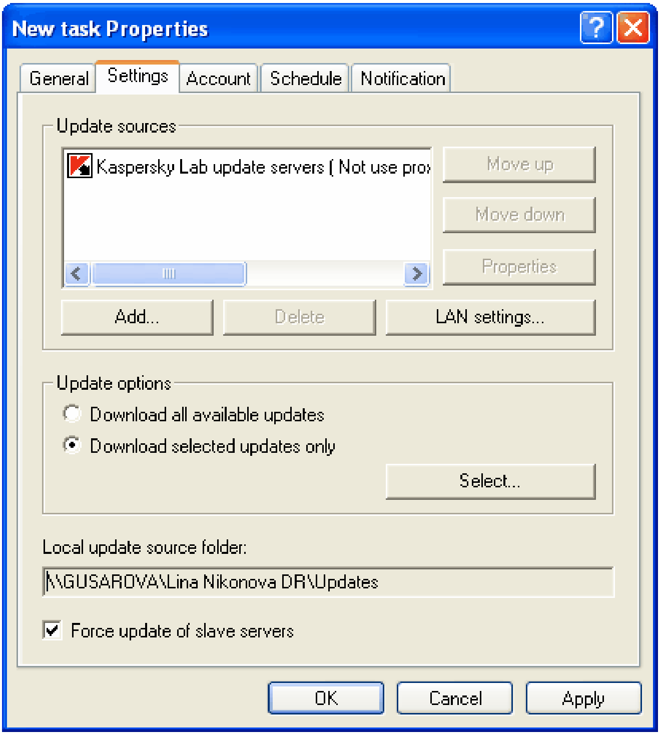

New task wizard
Select application
Select application to perform the task
Application
Name
Kaspersky Administration Kit
Kaspersky Network Agent
Kaspersky Anti-virus for MS Exchange Server
Kaspersky Anti-virus for MS Exchange Server
Task type
Name
Download updates task
Create backup of Admistration Server
Send report to e-mail recipient
Product deinstallation task
Product deployment task
< Back
Next >
Cancel
Help

Figure 20. Creating an updating task. Selecting application and task type

If the Administration server hierarchy is created (or is planned to be created) in the logical network, then the **Force the updating of the slave servers** box (see Figure 21) must be checked in the task settings on the main Server in order to ensure automatic distribution of the updates to the slave Servers. In this case, immediately after the update of the main Server updating tasks of the slave Servers (if such tasks have been created) will be launched.

If the **Enforce the updating of the slave servers** box is checked, automatic creation of tasks for receiving updates by the slave Administration server will not be performed. These tasks must be manually created for each slave Server individually.



Update sources

Kaspersky Lab update servers (Not use prox

Update options

○ Download all available updates

● Download selected updates only

Local update source folder:

\\GUSAROVA\Lina Nikonova DR\Updates

☑ Force update of slave servers

Figure 21. Configuring the task for receiving updates:

As the result of the execution of the task for receiving updates by the Administration server, the anti-virus database and the application modules updates will be downloaded from the updates source and placed into the public access folder.

From the public access folders the downloads will be distributed to the client computers (see section 5.2 on page 62) and slave Administration servers (see section 5.3 on page 65).

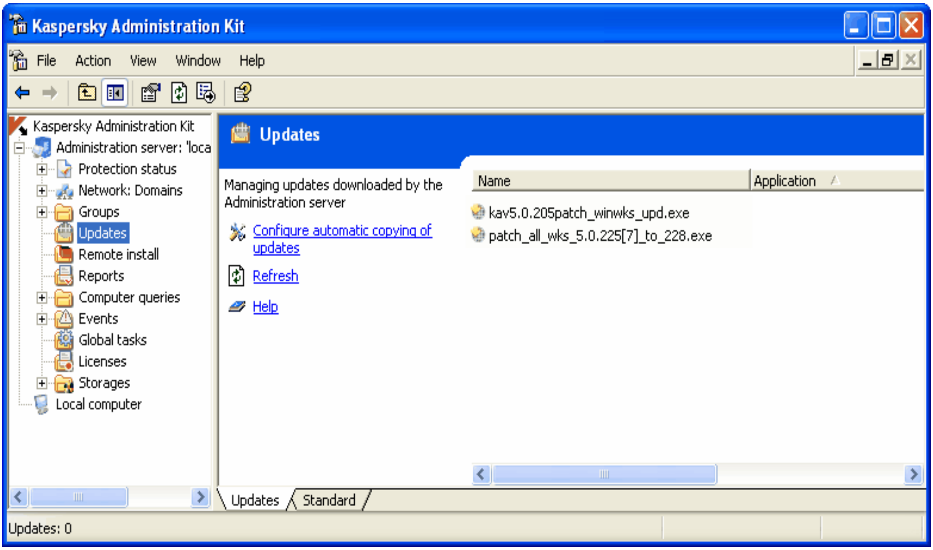
The following resources can be used as the update source for the Administration server:

- Kaspersky Lab's updates servers;
- Main Administration server;
- ftp- / http server or the network updates folder.

The use of the particular resource depends on the task settings.

> If the updates are performed from ftp- /http- servers or from the network folder, then in order to ensure correct updating of the server the structure of the folders with updates matching the structure created by the Kaspersky Lab's tools when the updates are copied, must be copied to these resources.

You can review information about received updates in the Updates container of the console tree; the list of updates is displayed in the results pane (seeFigure 22).



Managing updates downloaded by the Administration server

kav5.0.205patch_winwks_upd.exe

patch_all_wks_5.0.225[7]_to_228.exe

Updates: 0

Figure 22. Viewing the received updates

5.2. Distribution of updates to the client computers

5.2.1. Updates using the application tools

In order to increase the reliability of the anti-virus protection the tasks for receiving updates shall be created for all anti-virus applications included into the anti-virus protection system of the computers within the logical network.

In order to ensure that anti-virus database and application modules updates versions installed on the client computers within the logical are the same, select the Administration server as the updates source in the settings of the tasks for receiving updates by the applications.

If the Administration server is selected as the updates source in the application updating task, then, given the hierarchal structure of the Servers, the client computers will be updated from the server to which they are connected, that is from the slave server rather than from the main server.

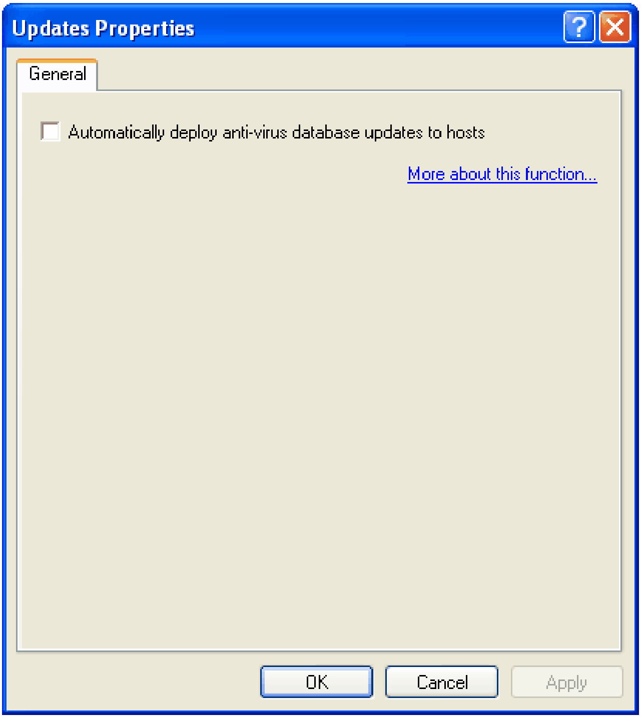
The procedure used to create the application updating tasks is described in the Guides for the corresponding applications.

5.2.2. Automatic distribution of the updates by the Administration server

The remote administration system provides a possibility to automatically distribute updates to the client computers with Kaspersky Anti-Virus for Windows Workstations versions 5.0 and 6.0, Kaspersky Anti-Virus 5.0 for Windows File Servers and Kaspersky Anti-Virus 6.0 for Windows Servers installed immediately after these updates have been received by the Administration servers.

In order to ensure it, box **Automatically deploy anti-virus database updates to hosts** in the properties of the **Updates** node must be checked (see Figure 23).

If this box is checked, then after each receipt of the updates by the **Administration server** four special tasks will be created in the **Group tasks** folder of the **Groups** group: **Automatic updating - Anti-Virus signagures** (one for each application). These tasks will be launched automatically after each successful receipt of the updates by the Server. In order to disable the mode of automatic distribution of the updates (box is unchecked), the tasks will be deleted.



Updates Properties

General

□ Automatically deploy anti-virus database updates to hosts

More about this function...

Figure 23. Configuration of automatic updating of the client computers

We recommend that you use automatic distribution of updates in order to decrease the traffic and the number of client computers' calls to the Administration server and in order to avoid mistakes and errors when creating the update tasks for the logical networks with a large number of client computers.

If the structure of the Administration servers is hierarchal, the mode of automatic updates distribution to the client computers must be enabled only for the main Administration server. Tasks **Automatic updating – Anti-virus Signatures** will be distributed in the client computers of the slave Servers based on the existing hierarchy.

If the structure of the Administration server is hierarchal, the tasks of automatic updating to the client computers of the slave Servers will be updated after the successful updating of the Server to which they are connected, that is the slave server, rather than the main server.

In the settings of the **Automatic updating - Anti-virus Signatures** task the Administration server was selected as the updates source. In order to ensure that the client computers of the slave Servers receive updates in timely fashion using this task, you have to enable the mode of automatic updating of the slave Servers in the settings of the main Server updating task.

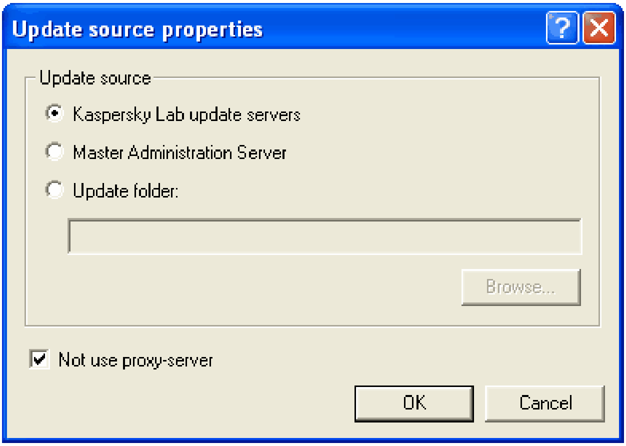
In order to decrease the load on the Administration servers we recommend that you use the updating agents that would ensure distribution of the updates within the administration group.

5.3. Updating of the slave Servers and their client computers

If hierarchal structure of the Administration servers is arranged in the logical network, then in order to ensure that the slave Servers receive the updates and distribute them to the client computers connected to them, you should:

- create a task for receiving updates for each slave Administration server.
- Select **Main Administration Server** as the updates source in the settings of the task for receiving updates for the slave Servers.
- •Enable mode of automatic updates distribution to the slave Servers in the settings of the tasks for receiving updates by the main Administration server: check the **Force the updating of the slave servers** box (see Figure 24).
- If required, indicate the updating agents within the administration groups (see section 5.4 on page 66).
- Enable the mode for automatic updates distribution to the client computers with Kaspersky Anti-Virus for Windows Workstations versions 5.0 and 6.0, Kaspersky Anti-Virus 5.0 for Windows File Servers and Kaspersky Anti-Virus 6.0 for Windows Servers installed; for other applications create or configure tasks for receiving updates from the Administration servers.

  Updates are received by the applications from the Administration servers to which the client computer is connected, that is from the slave Server rather than the main Server.



Update source properties

Update source

● Kaspersky Lab update servers

○ Master Administration Server

○ Update folder:

☑ Not use proxy-server

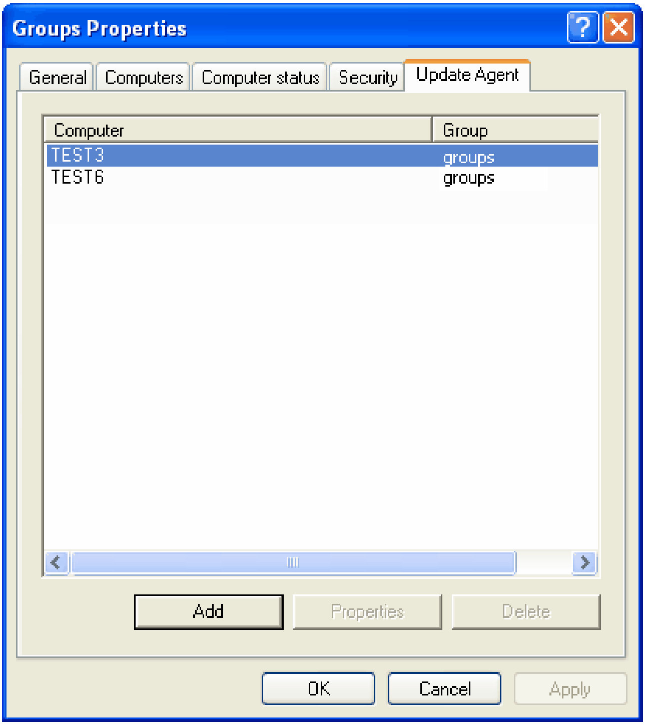
Figure 24. Updating from the main Administration server

5.4. Updates distribution using the updating agents

In order to distribute the updates to the client computers in the group you can use *updating agents* - computers that act as intermediate centers for distributing updates and installation packages within administration groups. They receive updates from the Administration server and place them into the application installation folder. Only those updates that are required within the group are downloaded. Later client computers within the group can use the agents to download updates using SSL connection.

Changes of the location of the folder that contains the updates and installation packages or imposing restrictions on its size is not allowed.

Creation of the updating agents list and their configuration are performed in the group's properties window on the **Updating agents** tab (see Figure 25).



Computer	Group
TEST3	groups
TEST6	groups

Figure 25. Creating the list of updating agents

CHAPTER 6. MAINTENANCE

6.1. Renewing your license

The right to use Kaspersky Lab's software is granted based on the license agreement entered into when you purchase the software product.

During the licensing period, you can:

- Use the anti-virus functionality of the application
- Update the anti-virus database
- Upgrade the versions of this application
- Receive technical support on matters related to the installation, configuration, and operation of this anti-virus application by phone or via a web-form used for inquiries to Technical support service and located at the Kaspersky Lab's corporate website.
- Send suspicious and infected objects to Kaspersky Lab for expert analysis

The program you installed automatically checks for the license agreement and determines the licensing period using a license key that is a part of every Kaspersky Lab application. An application can have only one valid license key. The license key contains terms for using the software that can be read and verified by special program means.

After the licensing term is over, you are unable to use the options listed above. To renew the license, you should purchase and install a new license key.

Kaspersky Administration Kit helps you centrally monitor the validity of and renew license keys installed on clients across your corporate logical network.

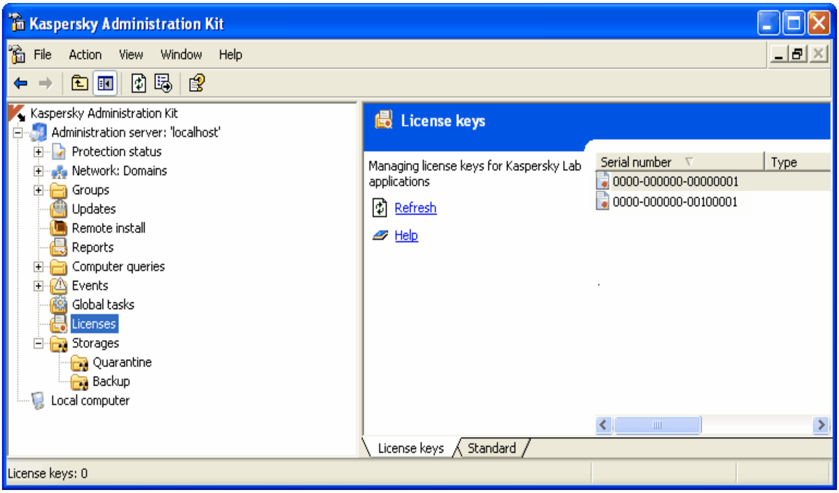
When a license key is installed using Kaspersky Administration Kit, the information about this license key is stored on the administration server. This information is used to create reports on license status and notify the administrator if the license is about to expire or the maximum number of permitted uses is exceeded. Parameters of notifications about the status of the license keys can be edited in the Administration server settings.

In order to create a report about the status of the license keys installed on the client computers within the logical network, you may use an in-built template **Report about license keys** or create a new template of the type that has the same name.

The report created using the **Report about license keys** template contains complete information about all license keys installed on the client computers within the logical network, including both current and backup license keys, with the indication of the computers on which they are used and the license restrictions.

A full list of license keys installed on clients is shown in the **Licenses** node. The following data is available for each key:

- **Serial number** – License key serial number
- **Type** – Type of the license key (for example, **commercial or trial)**
- **Limit** – License restrictions imposed by the license key
- **License period** – License key expiration period



Managing license keys for Kaspersky Lab applications

Serial number	Type
0000-000000-00000001	
0000-000000-00100001	

Figure 26. License keys

To view information about what license keys are installed for an application on a specific client, open the application properties dialog box.

To install a license key, you should create an **Install license key** task.

The Install license key task can be a group task, a global task, or a local task. You can create a global task to install license key using the wizard.

In order to replace the installed license key or install a license key as the current key, you can use a task you created earlier by changing its settings before using it.

6.2. Quarantine and backup storage

Working with quarantine and backup storage is available only for Kaspersky Anti-Virus for Windows Workstations and Kaspersky Anti-Virus for Windows Servers versions 5.0 and 6.0.

Anti-virus applications allow storing objects in specialized storage areas. For each computer there is a provision for individual quarantine and backup storage folders arranged locally on each computer. The quarantine storage is used to place suspicious objects while the backup storage - backup copies of infected objects before such objects are treated or deleted.

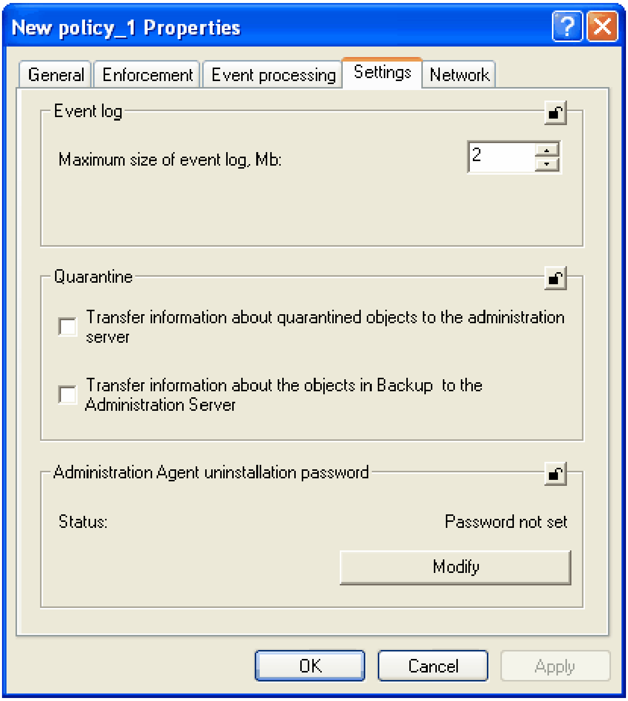
The Kaspersky Administration Kit application provides for the ability to maintain a centralized list of objects placed into storage areas by the Kaspersky Lab's applications. This information is transferred from the client computers by the Network Agents and stored in the Administration server's information database. There is an ability to perform the following functions via the Administration console: view properties of objects located in the storage areas, launch the anti-virus scan of storages and delete objects from these storages.

In order to activate the function of remote management of the local storage objects you must check the Transfer information about quarantined objects to the Administration server box and Transfer information about objects placed into the backup storage to the Administration server box (see Figure 27) in the policy for the Network Agent.

> The storage settings are defined individually for each application: in the policy or in the application settings.

You can view objects located in the storage areas of the client computers of the logical network and manage objects using the **Storages** folder (see Figure 28).

> Kaspersky Administration Kit does not copy objects to the Administration server. All objects are located in local storage areas on the client computers.
>
> The objects are restored to the folder specified in the administrator in the computer where the *Administration Console* is installed.



New policy_1 Properties

General | Enforcement | Event processing | Settings | Network

Event log

Maximum size of event log, Mb: 2

Quarantine

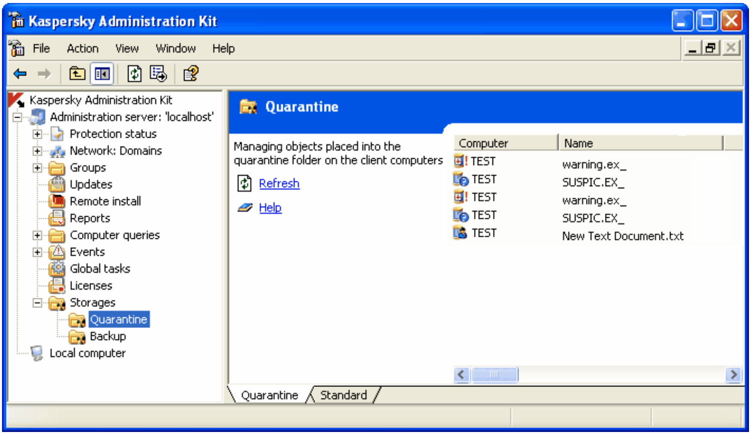
□ Transfer information about quarantined objects to the administration server

□ Transfer information about the objects in Backup to the Administration Server

Administration Agent uninstallation password

Status: Password not set

Figure 27. Configuring remotes storage areas



Kaspersky Administration Kit

- Kaspersky Administration Kit
  - Administration server: 'localhost'
    - Protection status
    - Network: Domains
    - Groups
    - Updates
    - Remote install
    - Reports
    - Computer queries
    - Events
    - Global tasks
    - Licenses
    - Storages
      - Quarantine
      - Backup
  - Local computer

Quarantine

Managing objects placed into the quarantine folder on the client computers

Computer	Name
TEST	warning.ex_
TEST	SUSPIC.EX_
TEST	warning.ex_
TEST	SUSPIC.EX_
TEST	New Text Document.txt

Figure 28. Viewing the storage contents

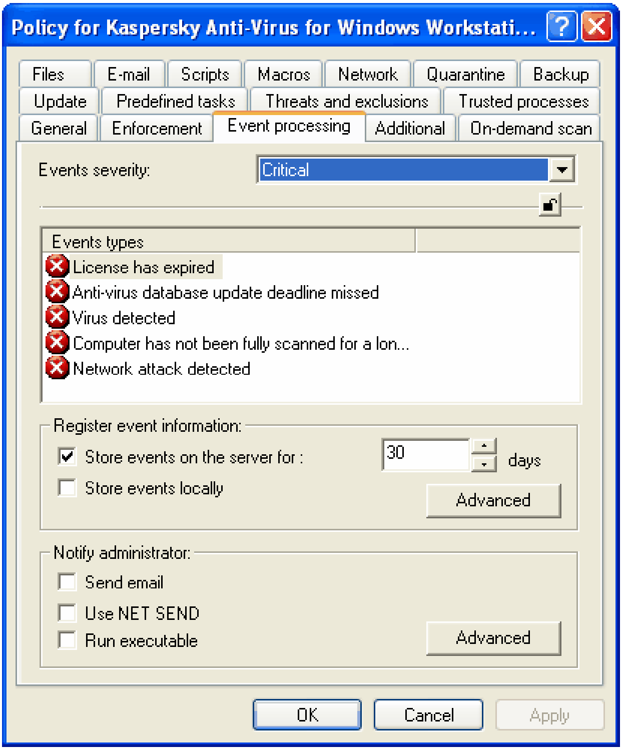
6.3. Event logs. Event filters.

Kaspersky Administration Kit application provides the user with various options of monitoring the operation of the anti-virus protection system.

There is a provision for maintaining event logs about the operation of the Administration server and all applications managed using Kaspersky Administration Kit. Data can be saved either in the Microsoft Windows system log or in the Kaspersky Administration Kit event log.

The log will contain events registered during the operation of the application and the results of tasks execution.

You can setup the list of events registered in the operation of each application and the procedure for providing notifications about them to the administrator and other users for each administration group. These parameters are determined by the application group policy. They are configured on the **Events** tab in the group policy window settings window (see Figure 29).



Events severity: Critical

Events types
- License has expired
- Anti-virus database update deadline missed
- Virus detected
- Computer has not been fully scanned for a lon...
- Network attack detected

Register event information:

☑ Store events on the server for : 30 days

□ Store events locally

Advanced

Notify administrator:

□ Send email

□ Use NET SEND

□ Run executable

Advanced

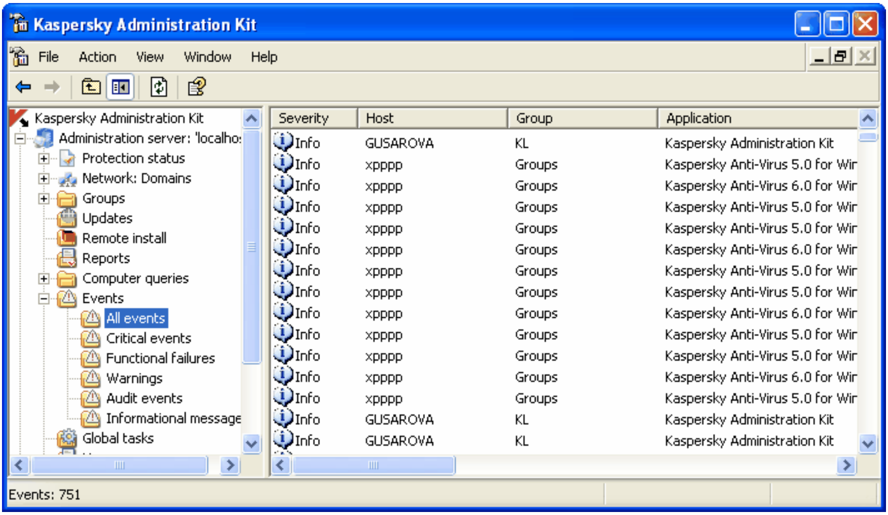
Figure 29. Editing policy. The **Events** tab.

The procedure used for saving the task execution results, the form and the method of notification about them is determined in the task settings.

The notification can be performed by sending message by e-mail or via the network or by launching a certain application or a script.

Information about registered events and results of task execution may be stored in a centralized location on the Administration server or, for each client computer, locally on the computer.

You can view information saved in the Microsoft Windows event log using standard MMC tool **Events viewer**. You can view the event log of Kaspersky Administration Kit saved on the Administration server using the **Events** node of the console tree (see Figure 30).



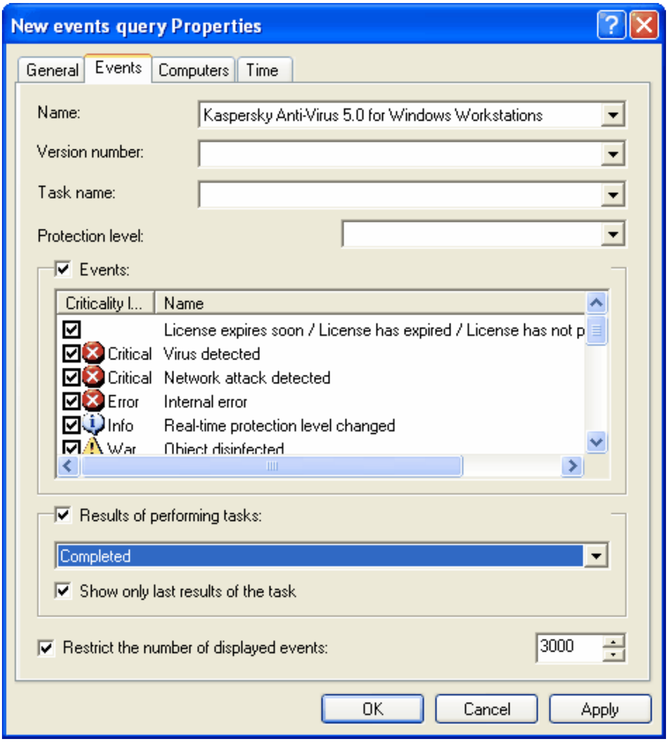
Severity	Host	Group	Application
Info	GUSAROVA	KL	Kaspersky Administration Kit
Info	xpppp	Groups	Kaspersky Anti-Virus 5.0 for Wir
Info	xpppp	Groups	Kaspersky Anti-Virus 6.0 for Wir
Info	xpppp	Groups	Kaspersky Anti-Virus 5.0 for Wir
Info	xpppp	Groups	Kaspersky Anti-Virus 5.0 for Wir
Info	xpppp	Groups	Kaspersky Anti-Virus 6.0 for Wir
Info	xpppp	Groups	Kaspersky Anti-Virus 5.0 for Wir
Info	xpppp	Groups	Kaspersky Anti-Virus 5.0 for Wir
Info	xpppp	Groups	Kaspersky Anti-Virus 6.0 for Wir
Info	xpppp	Groups	Kaspersky Anti-Virus 5.0 for Wir
Info	xpppp	Groups	Kaspersky Anti-Virus 5.0 for Wir
Info	xpppp	Groups	Kaspersky Anti-Virus 6.0 for Wir
Info	xpppp	Groups	Kaspersky Anti-Virus 5.0 for Wir
Info	GUSAROVA	KL	Kaspersky Administration Kit
Info	GUSAROVA	KL	Kaspersky Administration Kit

Events: 751

Figure 30. Viewing information of the Kaspersky Administration Kit event log

In order to simplify searching and viewing, information in the **Events** log is distributed by filtered layers corresponding to the level of importance of the event: **Critical events**, **Functional failures**, **Warnings**, **Informational messages**. The use of filters allows performing search and structuring of the information about registered events since after applying the filter only information complying with the filter parameters becomes available. This feature becomes very important in view of the amount of information stored on the Server. There is a possibility to create additional filters and save events in the .txt format file. For viewing all events and results of task execution, select the **All events** folder.

In order to create a filter, use the **New / New filter** item from the shortcut menu for the **Events** node. As the result a new folder with the name you have specified for the filtered results in the **Events** node of the console tree. This folder will contain all events and results for performing the task. In order to modify the information, configure the filter parameters (see Figure 31).



Name: Kaspersky Anti-Virus 5.0 for Windows Workstations

Version number:

Task name:

Protection level:

☑ Events:

	Criticality l...	Name
☑		License expires soon / License has expired / License has not p
☑	Critical	Virus detected
☑	Critical	Network attack detected
☑	Error	Internal error
☑	Info	Real-time protection level changed
☑	War	Object disinfected

☑ Results of performing tasks:

Completed

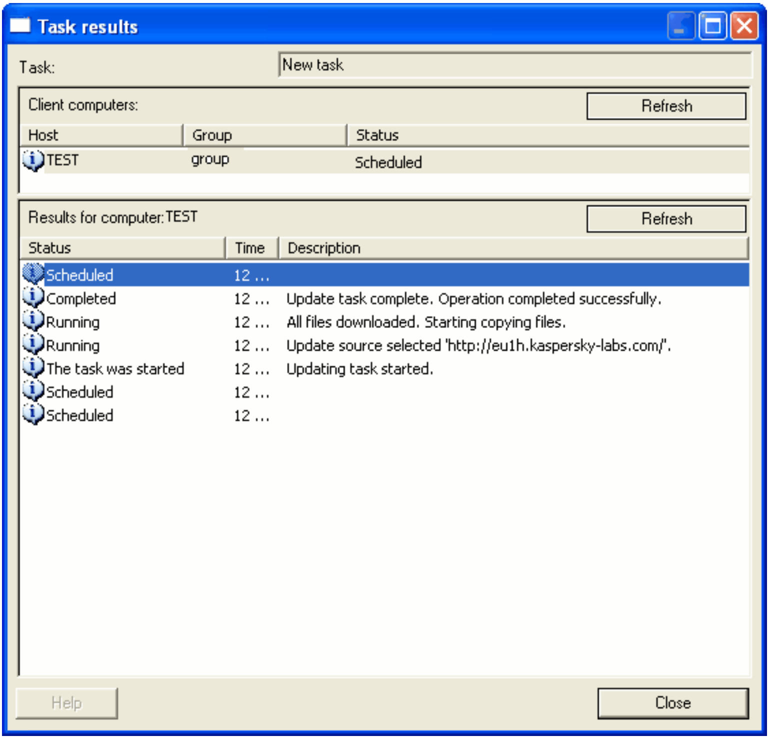
☑ Show only last results of the task

☑ Restrict the number of displayed events: 3000

Figure 31. Configuring an event filter

Registered events are deleted automatically after the expiration of the storage period specified by the policy or manually using the shortcut command menu **Purge.** You can delete an individual event selected in the results pane, all events or events that satisfy certain conditions.

You can review the list of events registered during the application operation for each client computer in its property window (see Figure 32). It displays information of the Kaspersky Administration Kit event log stored on the Administration server. In order to search for information, you can use the event filter.



Task: New task

Client computers:

Host	Group	Status
TEST	group	Scheduled

Results for computer: TEST

Status	Time	Description
Scheduled	12 ...	
Completed	12 ...	Update task complete. Operation completed successfully.
Running	12 ...	All files downloaded. Starting copying files.
Running	12 ...	Update source selected 'http://eu1h.kaspersky-labs.com/'.
The task was started	12 ...	Updating task started.
Scheduled	12 ...	
Scheduled	12 ...	

Figure 32. Viewing events stored on the Administration server

The Kaspersky Administration Kit event log stored locally on a client computer can be viewed via a local Administration Console installed on this computer.

6.4. Reports

You can receive reports about the status of the anti-virus protection system based on the information stored on the Administration server. Reports can be created for:

- the anti-virus protection system in general;
- computers included into a certain administration group;
- a set of client computers within various administration group;
- anti-virus protection system of the logical networks of the slave Administration servers.

The following reports can be generated:

- **Anti-virus database version report -** contains information about version of the anti-virus database used by the applications.
- **Errors report** - contains information about errors (functional failures) registered during the operation of applications installed on the client computers.
- **License key reports -** contains information about the status of the license keys used by the applications and about observing the restrictions imposed by these licenses.
- **Report on most infected client computers** - includes information about client computers on which the greatest number of suspicious and infected objects has been detected.
- **Anti-virus protection level report** - contains information about client computers with insufficient level of the anti-virus protection.
- **Kaspersky Lab's installed applications' versions report** - includes information about versions of Kaspersky Lab's applications installed on the client computers.
- **Virus activities report** - contains information about the results of the anti-virus scan of the client computers within the logical network.
- **Third-party application report -** contains information about third party software or Kaspersky Lab's applications not supporting administration via Kaspersky Administration Kit that are installed on the client computers.
- **Report about network attacks -** contains information about network attacks registered on the client computers.

You can generate reports based on templates previously created. Report templates are located in the **Reports** container of the console tree (see Figure 33).

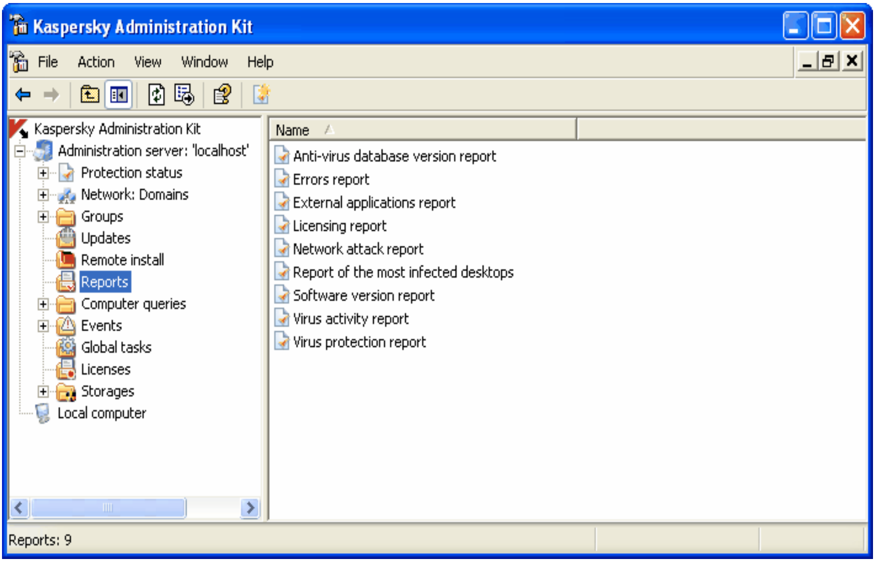


Figure 33. Viewing task execution results stored on the Administration server

There is a provision for nine (9) standard templates that match the corresponding types of reports about the anti-virus protection status.

You can create new templates, delete existing templates, view or edit their parameters.

Reports are viewed using the default browser.

In case of a hierarchal structure of the Administration server, you can create general reports, that would include information from the slave Administration servers.

If some Administration servers are not available, information about it will be contained in the report.

6.5. Finding computers

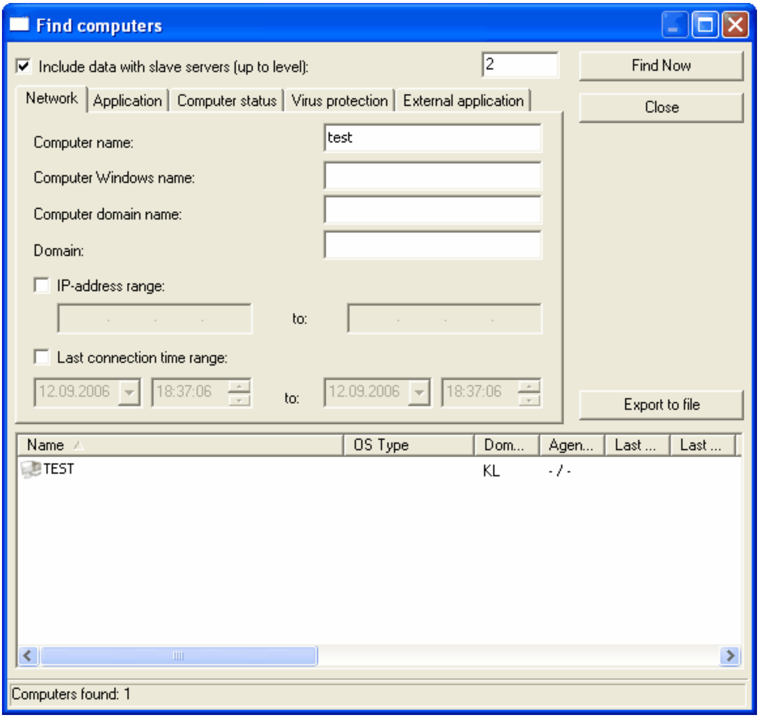
In order to receive information about a specific computer or a group of computers you can use the find computers function based on the specified criteria. Information from the slave Administration servers can be used in the search. The search results can be saved to a text file.

The search function allows finding:

- client computers within the logical network of the Administration servers or its slave Servers;

- computers not included into a logical network but included into the structure of computer networks where the Administration server and its slave Servers are installed;
- all computers within networks in which the Administration server and its slave Servers are installed irrespective of whether the particular computer is included into the structure of the logical network

For finding computers use the **Find computer** command from the shortcut menu for the Administration server node, **Network** folder or administration group selected in the console tree (see Figure 34).



☑ Include data with slave servers (up to level): 2

Computer name: test

Computer Windows name:

Computer domain name:

Domain:

☐ IP-address range: . . . to: . . .

☐ Last connection time range: 12.09.2006 18:37:06 to: 12.09.2006 18:37:06

Name	OS Type	Dom...	Agen...	Last ...	Last ...
TEST		KL	- / -		

Computers found: 1

Figure 34. Finding computers

Depending on the node for which the search is performed, the results of the search may be as follows:

- **The Group group**– a search for client computers connected to the logical network of the Administration server into which the selected group is included.

  The search is performed based on the information about the logical network structure and networks of the slave Administration servers (if the **In-**

clude data from the slave Servers box is checked in the search parameters).

- The **Network** group – search for computers within the network in which the Administration server not included into the logical network structure is installed.

  The search is performed based on the data obtained as the result of the polling of the computer network by the Administration server and the slave Servers (if the **Include data from the slave Servers** box is checked in the search parameters).

  The search results will include client computers included into the **Network** group selected for the search and in the **Network** groups of all slave Servers (if the **Include data from the slave Servers** box is checked in the search parameters).

- **Administration server <server name>** – full search for computers.

  The search is performed based on the information about the logical network structure and data obtained as the result of the polling of the computer network by the selected Administration server and the slave Servers (if the **Include data from the slave Servers** box is checked in the search parameters).

  The search results will include:

  - client computers of the logical network of the selected Administration server and all its slave Servers (if the I**nclude data from the slave Servers** box is checked in the search parameters).
  - computers of the Network group of the selected Administration server and of the **Network** groups of all its slave Servers (if the I**nclude data from the slave Servers** box is checked in the search parameters).

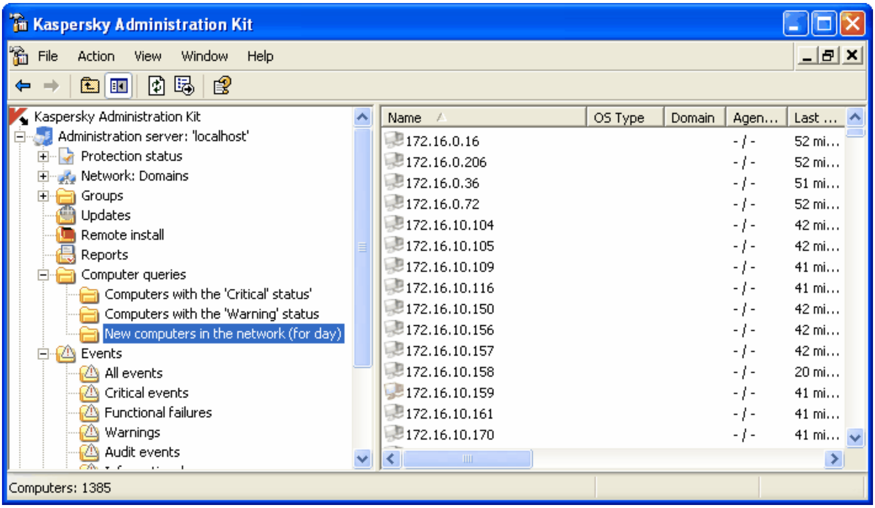
In order to search for, save and display information about computers in a separate folder of the console tree use the create filters function.

6.6. Computers filters

To ensure a more flexible monitoring of the status of the client computers within the logical network, information about computers with the **Critical** and **Warning** status and about computers detected in the network during the last 24 hours is presented in a separate node of the console tree named **Computer selections** (see Figure 35).

Diagnostics of the status of the client computers is performed based on the information about the anti-virus protection status on the computer and information about its activity in the network. Diagnostics settings parameters are configured for each administration group individually on the **Computer status** tab (see Figure 36).

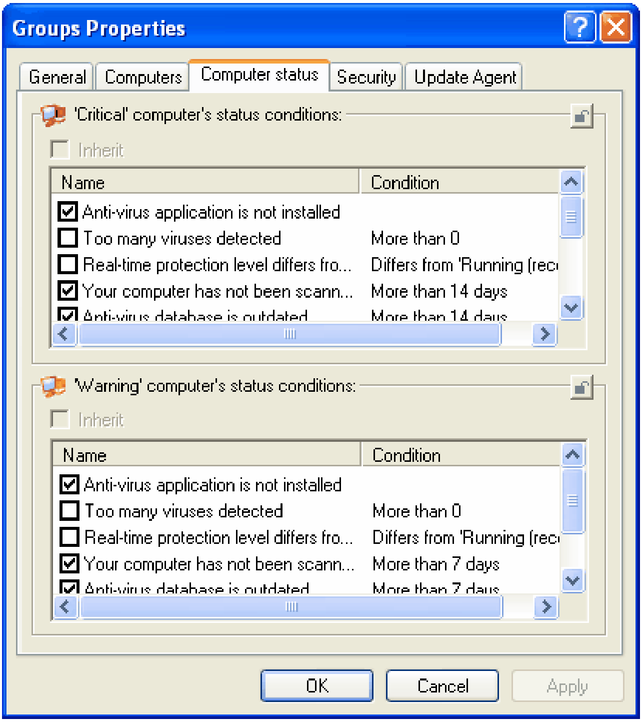
Information about new computers is provided based on the results of the poll of the computers network by the Administration server.


Kaspersky Administration Kit
File
Action
View
Window
Help
Kaspersky Administration Kit
Administration server: 'localhost'
Protection status
Network: Domains
Groups
Updates
Remote install
Reports
Computer queries
Computers with the 'Critical' status'
Computers with the 'Warning' status
New computers in the network (for day)
Events
All events
Critical events
Functional failures
Warnings
Audit events

Name	OS Type	Domain	Agen...	Last ...
172.16.0.16			- / -	52 mi...
172.16.0.206			- / -	52 mi...
172.16.0.36			- / -	51 mi...
172.16.0.72			- / -	52 mi...
172.16.10.104			- / -	42 mi...
172.16.10.105			- / -	42 mi...
172.16.10.109			- / -	41 mi...
172.16.10.116			- / -	41 mi...
172.16.10.150			- / -	42 mi...
172.16.10.156			- / -	42 mi...
172.16.10.157			- / -	42 mi...
172.16.10.158			- / -	20 mi...
172.16.10.159			- / -	41 mi...
172.16.10.161			- / -	41 mi...
172.16.10.170			- / -	41 mi...

Computers: 1385

Figure 35. Computers selections



'Critical' computer's status conditions:

☐ Inherit

Name	Condition
☑ Anti-virus application is not installed	
☐ Too many viruses detected	More than 0
☐ Real-time protection level differs fro...	Differs from 'Running (rec
☑ Your computer has not been scann...	More than 14 days
☑ Anti-virus database is outdated	More than 14 days

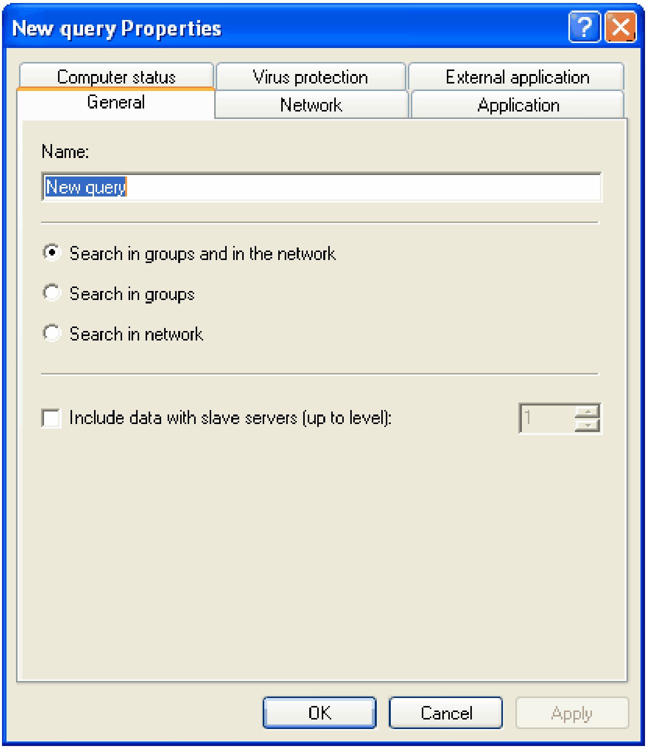
'Warning' computer's status conditions:

☐ Inherit

Name	Condition
☑ Anti-virus application is not installed	
☐ Too many viruses detected	More than 0
☐ Real-time protection level differs fro...	Differs from 'Running (rec
☑ Your computer has not been scann...	More than 7 days
☑ Anti-virus database is outdated	More than 7 days

Figure 36. Client computer diagnostic settings

There is a provision for creating additional filters. In order to create a filter, use the **New / New filter** item from the shortcut menu for the **Computer filters** node. As the result a new folder with the name you have specified for the filter will appear in the console tree will appear in the **Computer Selections** in the console tree. In order to add computers to the selection, configure the filter parameters (see Figure 37). The selection can be used for searching and further movement of selected computers into the administration groups. Movement is performed using a mouse.



New query Properties

Name: New query

● Search in groups and in the network
○ Search in groups
○ Search in network

□ Include data with slave servers (up to level): 1

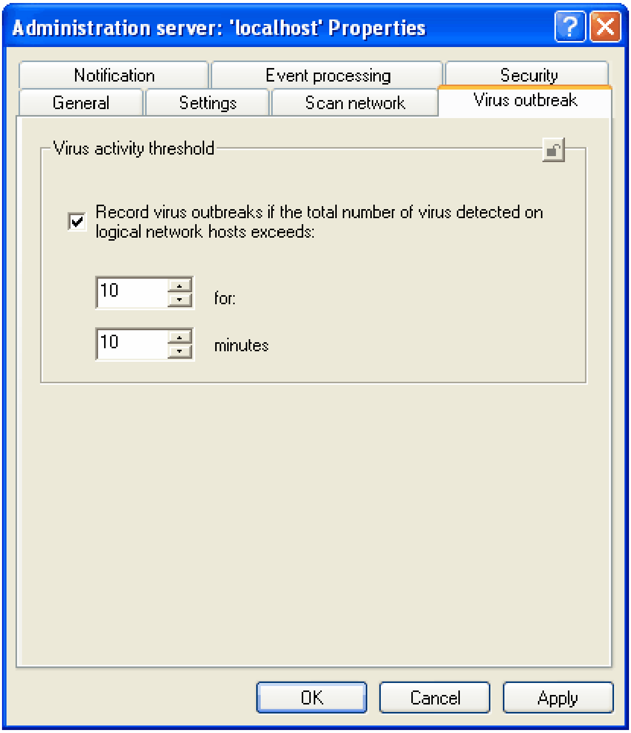
Figure 37. Configuring a computer filter

6.7. Virus outbreaks monitoring

Kaspersky Administration Kit allows monitoring the virus activities on the client computers within the logical networks using the **Virus attack** event registered in the operation of the Administration server component.

This feature is of great significance in the periods of virus outbreaks as it helps timely react on the emerging threats of virus attacks.

Criteria used for registering the **Virus attack** event is configured in the Administration server settings on the **Virus attack** tab (see Figure 38).



Virus activity threshold

☑ Record virus outbreaks if the total number of virus detected on logical network hosts exceeds:

10 for:

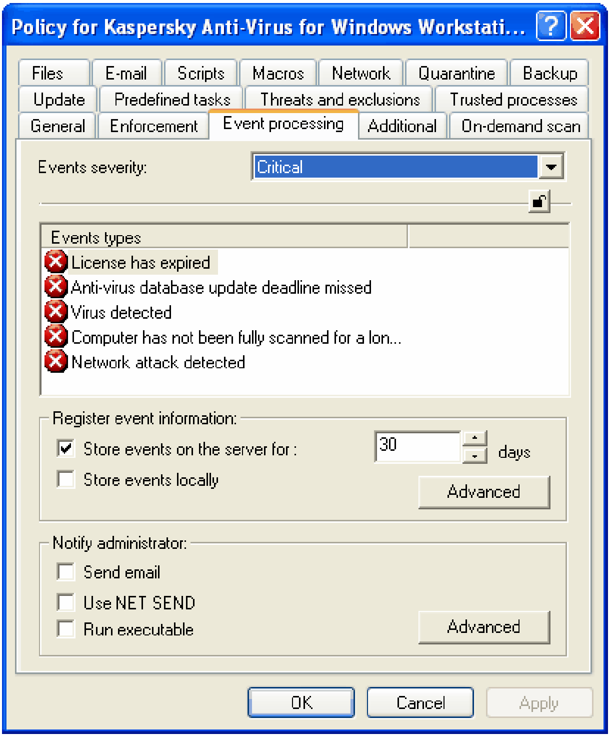
10 minutes

Figure 38. Configuring virus attack detection settings

In order to enable the virus attack detection mechanism check the **Register a virus attack if the total number of viruses detected on the computers within the logical network exceeds** box and specify the values for the parameters that determine the threshold of the virus activity level exceeding of which will be considered increased virus activities and will cause the **Virus attack** event.

Event **Virus attack** is created based on the **Virus detected** event in the operation of the anti-virus application. Therefore, in order to successfully detect virus outbreak all information about the **Virus detected** event must be stored on the Administration server. In order to do it the corresponding parameters in the policies for all anti-virus applications must be appropriately configured (box **Save on the Administration server** on the **Events** tab (see Figure 13) must be checked).

Event **Virus attack** cannot be created more than once in 24 hours. You can reset information about the occurrence of such event only be restarting the Administration server service.



Events severity: Critical

Events types	
☒ License has expired	
☒ Anti-virus database update deadline missed	
☒ Virus detected	
☒ Computer has not been fully scanned for a lon...	
☒ Network attack detected	

Register event information:

☑ Store events on the server for : 30 days

☐ Store events locally

Notify administrator:

☐ Send email

☐ Use NET SEND

☐ Run executable

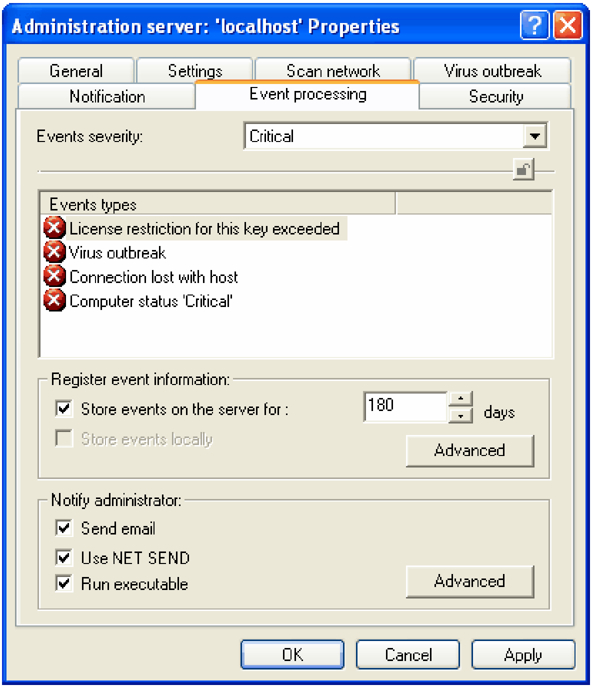
Figure 39. Configuring the event registration on the Administration server

The procedure for notification about event **Virus attack** is determined in the Administration server settings on the **Events** tab (see Figure 40).

Additionally, an automatic change of the current policy can be set as the reaction for the occurrence of the virus outbreak. In order to do it, the **Activate policy based on event** box must be checked in the policy settings and the **Virus attack** event (see Figure 11) must be selected.

For the purpose of counting events **Virus detected** only information from the client computers of the main Administration server is to be taken into account.

For each slave Server event **Virus attack** is configured individually.



Events severity: Critical

Events types	
☒ License restriction for this key exceeded	
☒ Virus outbreak	
☒ Connection lost with host	
☒ Computer status 'Critical'	

Register event information:

☑ Store events on the server for : 180 days

□ Store events locally

Notify administrator:

☑ Send email

☑ Use NET SEND

☑ Run executable

Figure 40. Configuring the settings for the notification of event

6.8. Backup copying and restoration of the Administration server data

Backup copying allows transferring the Administration server from one computer to another with no information loss and to restore data during the transfer of the information database of the Administration server to another computer or when upgrading to a new version of Kaspersky Administration Kit.

When the Administration server is removed from the computer Kaspersky Administration Kit always suggests to create a backup copy.

The following will be saved or restored during the backup copying:

- the Administration server information database (policies, tasks, application settings, events saved on the Administration server);

- configuration information about the structure of the logical network and client computers;
- storage of the applications' deployment packages (the content of the **Packages, Uninstall** and **Updates** folders);
- Administration server certificate.

Restoration of the data during the upgrading to a newer application version is supported starting with Kaspersky Administration Kit version 5.0 Maintenance Pack 3
If the path to the public folder has been changed while you were restoring data, make sure that the tasks that involve the shared folder run correctly (update tasks, deployment tasks) and, if necessary, modify the settings as required.

Copying data of the Administration server for the backup storage and its subsequent restoration can be performed automatically using the backup copying task or manually using the **klbackup** utility included into the distribution package of the Kaspersky Administration Kit. Data restoration is performed using the **klbackup** utility.

After the installation of the Administration server, the **klbackup** utility will be saved to the component installation folder and will copy or restore data (depending on the modifiers) when run from the command line.

The backup copying task is created automatically by the **Quick start wizard** and is located under name **Administration server** data backup copying in the **Global tasks** mode. In order to enable backup copying, you should configure this task's settings. You can also create a data backup copying task manually: As the application for which the task is created select **Kaspersky Administration Kit**, as the type of the task - **Receiving updates by the Administration server**.

APPENDIX A. GLOSSARY

This documentation uses some specific terms related to anti-virus protection. Glossary is a list of definitions of these terms. The glossary entries are arranged in alphabetical order to facilitate using the glossary.

A

Available updates – Service Packs that contain urgent updates accumulated over time and latest changes in the application architecture.

Administration group – Computers grouped in accordance with their functional and installed Kaspersky Lab applications. Grouping significantly facilitates the management process and allows the administrator to manage all computers as a single entity. A group might include other groups. Group policies and group tasks can be created for each application of installed on group members.

Administration Console– A Kaspersky Administration Kit component that provides user interface for the administrative services of the Administration Server and Network Agent.

Anti-virus database – A database created by Kaspersky Lab specialists that contains detailed definitions of all currently existing viruses and methods for their detection and disinfection. Anti-virus applications use the database to successfully detect and disinfect viruses. The anti-virus database available on the Kaspersky Lab websites is regularly updated as new virus threats appear. Registered users of Kaspersky Lab applications have access to database updates. To keep your computer constantly protected from viruses, we strongly recommend that you download updates on a regular basis.

Administrator workstation – A computer where the Administration Console of Kaspersky Administration Kit is installed. Using the Console, the administrator can build and manage the anti-virus protection system based on Kaspersky Lab applications.

Anti-virus protection status – Current status of anti-virus protection that characterizes the security level for your computer.

Administration Server – A Kaspersky Administration Kit component that centrally stores information about Kaspersky Lab applications installed on clients and manages these applications.

Administration Server certificate – A certificate used to authenticate the Administration Server upon connection of the Administration Console to the server and data transmission between the server and clients. The Administration Server certificate is created during the installation of the Administration Server. It is located in the **Cert** folder of the installation folder.

B

Block object – Prevent external applications from accessing an object. The blocked object cannot be read, executed, modified, or deleted.

Backing up – copying data of the Administration server for storage and subsequent restoration performed by the backup utility. The utility allows to save:Administration Server database that stores policies, tasks, application settings, and events logged on the Administration ServerInformation about the logical networks and client configurations Installation files for the remote installation of applications (contents of the Packages, Uninstall, Updates folders) Administration Server certificate

BACKUP folder – A directory that contains backups of deleted and disinfected objects.

Backup storage – A folder that contains the backup copies of Administration Server data created by the backup utility.

C

Console (management) plug-in – A special component that provides an interface for remotely managing an application through the Administration Console. The plug-ins are specific to each application and are included in all Kaspersky Lab applications that can be managed through Kaspersky Administration Kit.

Centrally managing an application – Managing an application through Kaspersky Administration Kit.

Client, Administration Server (or **client computer**) – a computer, a server, or a workstation with the installed Network Agent and managed Kaspersky Lab applications.

D

Disinfection – A method of treating infected objects. Disinfection implies partial or full recovery of data or results in a decision that these files cannot be disinfected. Objects are disinfected using the anti-virus database. If disinfection is the first action to be applied to an object, i. e. the first action after detection of a suspicious object, the program creates a backup of this file. If some data are lost during disinfection, you can use the backup to recover this object.

Deleting an object – A method of handling an object. To delete an object is to remove it physically from a computer. This method is recommended for treating infected objects. If deleting is the first action applied to an object, it is necessary to create a backup of this object before deleting it. You can use the backup to restore the original object.

E

Exclusions – User-defined settings that exclude certain objects from scans. You can customize the exclusion rules for *real-time protection* and *on-demand scans*. Thus, you can disable scanning of archives during a full scan or exclude files from scans by their masks.

E-mail databases – Databases that contain e-mail messages stored on your computer. Every incoming/outgoing message is saved in the database after you receive/send it. Such databases are scanned in the on-demand scanning mode.

G

Global task – A task defined for and running on a number of clients from different administration groups.

Group Task – A task defined for and running on all clients in a group.

Group policy – A set of application settings in an administration group managed through Kaspersky Administration Kit. Group policies can be different for each group. Group policies are specific to individual applications. The policy involves configuration of all parameters of applications.

I

IChecker technology – A technology that excludes the objects from future scans that remained unmodified since the last scan. The IChecker technology was implemented by using the object checksum database.

IStreams technology – A technology that excludes the files stored on NTFS-formatted disks that remained unmodified since the last scan. The IStreams technology was implemented by using a method of storing file checksums in the additional NTFS streams.

Infected object – An object containing a virus. We recommend that you abandon working on these objects because they can infect your computer.

Installation package – A package of files used to install Kaspersky Lab applications on remote hosts on a logical network. Installation packages are based on a special **.kpd** file included in the application distribution kit, which contains a minimum set of parameters that provide the basic functionality of the application immediately after the installation. The values of the parameters are default settings of the applications.

K

Kaspersky Lab update servers – A list of http and ftp Kaspersky Lab websites where you can copy updates to your computer from.

Kaspersky Administration Kit – An application for centralized performance of key administrative tasks. It gives you complete control over the enterprise anti-virus policy based on Kaspersky Lab applications.

L

License key – A file with the .*key* extension that serves as your personal "key". This file is required for correct operation of Kaspersky Lab applications. The license key is included in the distribution kit if you purchased your copy of the application from Kaspersky Lab distributors. If you purchased the application online, the license key is sent to you via e-mail. Without the license key, Kaspersky Anti-Virus DOES NOT WORK.

Logical network operator – A user that monitors the system of anti-virus protection managed by Kaspersky Administration Kit.

Local management – Management of an application through a local interface.

Local task – A task created for and running on a single client.

License period – A period during which you have the right to take advantage of the full functionality of Kaspersky Anti-Virus. As a rule, the license period defined by the license key is one year from the date of purchase. After your license expires, the application will operate but you will not be able to update the *anti-virus database*.

Local network administrator – A user who installs, configures, and maintains Kaspersky Administration Kit and remotely manages Kaspersky Lab applications installed on the logical network computers.

M

Maximum protection – A protection level that ensures comprehensive protection but slightly decreases performance characteristics.

Maximum speed – A protection level that has a maximum operation speed but a lower security level.

N

Network Agent – A Kaspersky Administration Kit component that provides communication between the Administration Server and Kaspersky Lab applications installed on specific network nodes (workstations or servers). This component is common to all applications included in Kaspersky Lab Business Optimal and Corporate Suite.

O

OLE-object – An object linked or embedded into other files by using OLE technology.

On-demand full scan – An administrator-defined mode that scans all files on your computer for viruses and disinfects/deletes infected objects upon their detection.

P

Policy – see **Group policy**

Push installation – A remote installation method that allows you to install Kaspersky Lab software on specified computers on your logical network. In order to successfully perform the task using a push installation, the account used to launch this task must have rights to run applications on remote clients. This method is recommended for computers running MS Windows NT/2000/2003/XP, which support this feature, or for computers that are running MS Windows 98/Me and have an installed Network Agent.

Q

Quarantining – A method of handling a *suspicious* object. Access to this object is blocked and the file is moved to the quarantine for further processing.

Quarantine – A special storage that isolates infected and suspicious objects.

R

Real-time protection – A scanning mode in which an anti-virus application is memory resident. In the real-time protection mode, the application scans all objects when you open them for reading, writing, or executing. Before enabling access to an object, Kaspersky Anti-Virus scans it for viruses and, if a virus is detected, blocks access to the object, disinfects it or deletes it (depending on user-defined settings).

Recommended level – The level of antivirus protection with default settings recommended by Kaspersky Lab experts which ensures the optimal protection of your computer. This level is set by default.

Remote installation– Installation of Kaspersky Lab applications using the services provided by Kaspersky Administration Kit.

Restoring – Restoring Administration Server data using a backup utility. The information for restoring is available in the backup storage. The utility allows you to restore: Administration Server database that stores policies, tasks, application settings, and events logged on the Administration Server Information about the logical networks and client configurations Installation files for the remote installation of applications (contents of the Packages, Uninstall, Updates folders) Administration Server certificate

S

Script-based installation – An installation method that relates the remote installation task with a specified user account (several accounts). When the specified user logs onto the domain, the application will be installed on the client where this user has logged on. This method is recommended for use with computers running MS Windows 95/98/Me

Settings, task – Application settings specific for each type of task.

Settings, applications – Application settings specific for all types of tasks performed by this application.

Severity level – A parameter that classifies an event recorded during Kaspersky Anti-Virus performance. There are four severity levels:

Critical

Error

Warning

Info

Events of the same kind can be of different severity levels, depending on a specific situation.

Startup objects – A set of programs that are necessary for launching and smooth operation of the operating system and other software installed on your computer. Your operating system launches these objects during each startup. Some viruses attempt to infect the startup objects and can cause a startup failure.

Suspicious object – An object that contains either a modified code of a well-known virus or a code reminiscent of a virus yet unknown to Kaspersky Lab specialists.

Scan files by format – In this scanning mode, the program analyzes the contents of a file, namely, the format identifier in the file header.

Scan files by extension – In the scanning mode, the program takes into account the scanned file extension.

T

Task – An action that has a name performed by a Kaspersky Lab application.

Third party application – An anti-virus application by a third-party vendor or a Kaspersky Lab's application not supporting administration via Kaspersky Administration Kit.

U

Unknown virus – A new virus that is not recorded in the *anti-virus database*. As a rule, Kaspersky Anti-Virus detects unknown viruses using an *heuristic code analyzer* and objects containing these viruses are identified as *suspicious*.

Updating – A function of Kaspersky Anti-Virus that updates/adds new files (anti-virus database or program modules) retrieved from Kaspersky Lab update servers.

Updating agents - computers that act as intermediate centers for distributing updates and installation packages within the administration groups.

V

Virtual drives (RAM drives) – A part of RAM emulating a normal physical disk of a personal computer.

Virus activity threshold – number of viruses detected for a specified time interval. When this number is exceeded, the situation is regarded as a **Virus outbreak** (virus attack). This parameter is important for defining virus epidemics because the administration can respond in a timely fashion to new threats and take preventive measures to protect his/her network.

APPENDIX B. KASPERSKY LAB

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, comprehensive solutions to protect computers and networks against all types of malicious programs, unsolicited and unwanted email messages, and hacker attacks.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has representative offices in the United Kingdom, France, Germany, Japan, USA (CA), the Benelux countries, China and Poland. A new company department, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network incorporates more than 500 companies worldwide.

Today, Kaspersky Lab employs more than 250 specialists, each of whom is proficient in anti-virus technologies, with 9 of them holding M.B.A. degrees, 15 holding Ph.Ds, and two experts holding membership in the Computer Anti-Virus Researchers Organization (CARO).

Kaspersky Lab offers best-of-breed security solutions, based on its unique experience and knowledge, gained in over 14 years of fighting computer viruses. A thorough analysis of computer virus activities enables the company to deliver comprehensive protection from current and future threats. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. At all times, the company's products remain at least one step ahead of many other vendors in delivering extensive anti-virus coverage for home users and corporate customers alike.

Years of hard work have made the company one of the top security software manufacturers. Kaspersky Lab was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company's flagship product, Kaspersky Anti-Virus, provides full-scale protection for all tiers of a network, including workstations, file servers, mail systems, firewalls and Internet-gateways, hand-held computers. Its convenient and easy-to-use management tools ensure advanced automation for rapid virus protection across an enterprise. Many well-known manufacturers use the Kaspersky Anti-Virus kernel, including Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada).

Kaspersky Lab's customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. Kaspersky Lab's anti-virus database is updated every 3 hours. The company provides its customers with a 24-hour technical support service, which is available in several languages to accommodate its international clientele.

B.1. Other Kaspersky Lab Products

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal has been designed to provide anti-virus protection to personal computers running Microsoft Windows 98/ME or Microsoft Windows 2000/NT/XP against all known viruses, including potentially dangerous software. Kaspersky Anti-Virus Personal provides real-time monitoring of all sources of virus intrusion - e-mail, internet, CD, etc. The unique system of heuristic data analysis allows efficient processing of yet unknown viruses. This application can work in the following modes (that can be used separately or jointly):

- **Real-time computer protection** - anti-virus scanning of all objects run, opened on or saved to the user's computer.
- **On-demand computer scan** - scan and disinfection of the entire user's computer or of individual disks, files or folders. You can start such scan manually or configure an automatic scheduled scan.

Kaspersky Anti-Virus® Personal does not re-scan objects that had been already scan during a previous scan and have not changed since then not only when performing real-time protection, but also during an on-demand scan. This **considerably increases the speed of the program's operation**.

The application creates a reliable barrier to viruses when they attempt to intrude your computer via e-mail. Kaspersky Anti-Virus® Personal performs automatic scan and disinfection of all incoming and outgoing mail sent or received using POP3 and STMP protocol and provides highly efficient detection of viruses in mail databases.

The application support over 700 formats of archived and compressed files and provides automatic scan of their content as well as removal of malicious code from **ZIP, CAB, RAR, ARJ, LHA and ICE** archives.

Configuring the application is made simple and intuitive due to the possibility to select of the preset protection levels: **Maximum Protection**, **Recommended** and **High Speed**.

The anti-virus database is updated every three hours and its delivery to your computer is guaranteed even when your computer gets temporarily disconnected from the internet or the connection has been changed.

Kaspersky Anti-Virus® Personal Pro

This package has been designed to deliver comprehensive anti-virus protection to home computers running Microsoft Windows 98/ME/2000/NT/XP as well as MS Office 2000 applications. Kaspersky Anti-Virus Personal Pro includes an easy-to-use application for automatic retrieval of daily updates for the anti-virus database and the program modules. A second-generation heuristic analyzer efficiently detects unknown viruses. Kaspersky Anti-Virus Personal includes many interface enhancements, making it easier than ever to use the program.

Kaspersky Anti-Virus® Personal Pro has the following features:

- **On-demand scan** of local disks;
- **Real-time automatic protection** of all accessed files from viruses;
- **Mail Filter** automatically scans and disinfects all incoming and outgoing mail for any mail client that uses POP3 and SMTP protocols and effectively detects viruses in mail databases;
- **Behavior blocker** that provides maximum protection of MS Office applications from viruses;
- **Archive scans –** Kaspersky Anti-Virus recognizes over 700 formats of archived and compressed files and ensures automatic anti-virus scanning of their content and removal of malicious code from files within **ZIP**, **CAB**, **RAR, ARJ, LHA and ICE** archives.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker is a personal firewall that is designed to safeguard a computer running any Microsoft Windows operating system. It protects your computer against unauthorized access and external hacker attacks from either the Internet or the local network.

Kaspersky® Anti-Hacker monitors the TCP/IP network activity of all applications running on your machine. When it detects a suspicious action, the application blocks the suspicious application from accessing the network. This helps deliver enhanced privacy and 100% security of confidential data stored on your computer.

The product's SmartStealth™ technology prevents hackers from detecting your computer from the outside. In this stealthy mode, the application works seamlessly to keep your computer protected while you are on the Web. The application provides conventional transparency and accessibility of information.

Kaspersky® Anti-Hacker also blocks most common network hacker attacks and monitors for attempts to scan computer ports.

Configuration of the application is simply a matter of choosing one of five security levels. By default, the application starts in self-learning mode, which will automatically configure your security system depending on your responses to various events. This makes your personal guard adjustable to your specific preferences and your particular needs.

Kaspersky® Personal Security Suite

Kaspersky® Personal Security Suite is a program suite designed for organizing comprehensive protection of personal computers running Microsoft Windows. The suite prevents malicious and potentially dangerous programs from penetrating through any possible data sources and protects you from unauthorized attempts to access your computer's data, as well as blocking spam.

Kaspersky Personal Security Suite has the following features:

- anti-virus protection for data saved on your computer;
- protection for users of Microsoft Outlook and Microsoft Outlook Express from spam;

- protection for your computer from unauthorized access, and also from network hacker attacks from your LAN or the Internet.

Kaspersky® OnLine Scanner

This program is a free service available to visitors of the corporate website allowing to perform efficient anti-virus scan of your computer and disinfection of infected files online. Kaspersky OnLine Scanner is executed in the web browser using the Microsoft ActiveX® technology. The users can quickly receive response to their concerns related to the infection with malware. While scanning the user can:

- exclude archives and mail databases from the scan scope;
- select standard / extended anti-virus database to be used for scanning;
- save reports with the scan results in txt and html format.

Kaspersky® OnLine Scanner Pro

This program is a subscription service available to visitors of the corporate website allowing to perform efficient anti-virus scan of your computer and disinfection of infected files online. Kaspersky OnLine Scanner Pro is executed in the web browser using the Microsoft ActiveX® technology. While scanning the user can:

- exclude archives and mail databases from the scan scope;
- select standard / extended anti-virus database to be used for scanning;
- save reports with the scan results in txt and html format.

Kaspersky® Security for PDA

Kaspersky® Security for PDA provides reliable anti-virus protection for data saved on various types of Pocket PCs and smartphones. The program includes an optimal set of anti-virus defense tools:

- **anti-virus scanner** that scans information (saved both on the PDA and smartphones) on user demand;
- **anti-virus monitor** to intercept viruses in files that are either copied from other handhelds or are transferred using HotSync™ technology.

Kaspersky® Security for PDA protects your handheld (PDA) from unauthorized intrusion by encrypting both access to the device and data stored on memory cards.

Kaspersky Anti-Virus® Business Optimal

This package provides a configurable security solution for small- and medium-sized corporate networks.

Kaspersky Anti-Virus® Business Optimal includes full-scale anti-virus protection[2] for:

[2] Depending on the type of distribution kit.

- Workstations running Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation and Linux;
- File servers running Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell Netware, FreeBSD and OpenBSD, Linux, Samba Servers;
- E-mail clients, namely Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail, and Qmail;
- Internet-gateways: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition.

The Kaspersky Anti-Virus® Business Optimal distribution kit includes Kaspersky® Administration Kit, a *unique tool for automated deployment and administration*.

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

Kaspersky® Corporate Suite

This package provides corporate networks of any size and complexity with comprehensive, scalable anti-virus protection. The package components have been developed to protect every tier of a corporate network, even in mixed computer environments. Kaspersky® Corporate Suite supports the majority of operating systems and applications installed across an enterprise. All package components are managed from one console and have a unified user interface. Kaspersky® Corporate Suite delivers a reliable, high-performance protection system that is fully compatible with the specific needs of your network configuration.

Kaspersky® Corporate Suite provides comprehensive anti-virus protection for:

- Workstations running Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstations and Linux;
- File servers running Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux and Samba Servers;
- E-mail clients, including Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim and Qmail;
- Internet-gateways: CheckPoint Firewall –1; Microsoft ISA Server 2004 Enterprise Edition;
- Hand-held computers (PDAs), running Microsoft Windows CE and Palm OS, and also smartphones running Microsoft Windows Mobile 2003 for Smartphone and Microsoft Smartphone 2002.

The Kaspersky® Corporate Suite distribution kit includes Kaspersky® Administration Kit, a *unique tool for automated deployment and administration*.

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam is a cutting-edge software suite that is designed to help organizations with small- and medium-sized networks wage war against the onslaught of undesired e-mail (spam). The product combines the revolutionary technology of linguistic analysis with modern methods of e-mail filtration, including RBL lists and formal letter features. Its unique combination of services allows users to identify and wipe out up to 95% of unwanted traffic.

Installed at the entrance to a network, where it monitors incoming e-mail traffic streams for spam, Kaspersky® Anti-Spam acts as a barrier to unsolicited e-mail. The product is compatible with any mail system and can be installed on either an existing mail server or a dedicated one.

Kaspersky® Anti-Spam's high performance is ensured by daily updates to the content filtration database by samples provided by the Company's linguistic laboratory specialists. Databases are updated every 20 minutes.

Kaspersky SMTP Gateway

Kaspersky® SMTP-Gateway for Linux/Unix is a solution designed for processing e-mail transmitted via SMTP for viruses. The application contains a number of additional tools for filtering e-mail traffic by name and MIME type of attachments and a series of tools that reduces the load on the mail system and prevents hacker attacks. DNS Black List support provides protection from e-mails coming from servers entered in these lists as sources for distributing e-mail.

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security for Microsoft Exchange performs the anti-virus scan of incoming and outgoing mail messages as well as messages stored at the server, including messages stored in the public folders and filters out unsolicited correspondence using "smart" anti-spam technologies in combination with Microsoft technologies. The application scans all messages arriving at Exchange Server via SMTP protocol for the presence of viruses, using Kaspersky Lab's anti-virus technologies and for the presence of SPAM attributes, filtering out spam using formal attributes (mail address, IP address, letter size, heading) and analyzing the content of the letter and of the attachments using "smart' technologies, including unique graphic signatures for identifying graphic SPAM. The scan includes both the body of the message and the attached files.

Kaspersky® Mail Gateway

Kaspersky Mail Gateway is a comprehensive solution that provides complete protection of the mail system users. This application installed between the corporate network and Internet scans all components of e-mail messages for the presence of viruses and other malware (Spyware, Adware, etc.) and performs centralized anti-spam filtration of the e-mail messages flow. This solution also includes some additional mail traffic filtration features.

B.2. Contact Us

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Lab. We will be glad to assist you in any matters related to our product by phone or via email. All of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at http://www.kaspersky.com/supportinter.html
General information	WWW: http://www.kaspersky.com http://www.viruslist.com Email: sales@kaspersky.com

APPENDIX C. LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”) FOR THE LICENSE OF SPECIFIED SOFTWARE (“SOFTWARE”) PRODUCED BY KASPERSKY LAB. (“KASPERSKY LAB”).

IF YOU HAVE PURCHASED THIS SOFTWARE VIA INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE LEGAL ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD'S SLEEVE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD's SLEEVE ,DOWNLOAD, INSTALL OR USE THIS SOFTWARE. IF YOU HAVE BROKEN THE CD'S SLEEVE OR OPENED THE BOX, YOU WILL NOT BE ENTITLED TO RETURN THE SOFTWARE FOR REFUND. SOFTWARE FOR HOME USE (KASPERSKY ANTI-VIRUS PERSONAL, KASPERSKY ANTI-VIRUS PERSONAL PRO, KASPERSKY ANTI-HACKER, KASPERSKY SECURITY FOR PDA) PURCHASED AS A DOWNLOAD VIA THE INTERNET MAY BE RETURNED FOR A FULL REFUND WITHIN 14 DAYS AFTER PURCHASE FROM KASPERSKY LAB, IT'S AUTHORIZED DISTRIBUTOR OR RESELLER. OTHER PRODUCTS ARE NON REFUNDABLE. THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

All references to “Software” herein shall be deemed to include the software activation key (“Key Identification File”) with which you will be provided by Kaspersky Lab as part of the Software.

1. License Grant. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby grants to you the non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the “Documentation”) for the term of this Agreement solely for your own internal business purposes. You may install one copy of the Software on one computer, workstation, personal digital assistant, or other electronic device for which the Software was designed (each, a “Client Device”). If the Software is licensed as a suite or bundle with more than one specified Software product, this license applies to all such specified Software applications, subject to any restrictions or

usage terms specified on the applicable price list or application packaging that apply to any such Software applications individually.

1.1 Use. The Software is licensed as a single application; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section.

1.1.1 The Software is “in use” on a Client Device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software’s proprietary notices. You will maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorized copying or use.

1.1.2 If you sell the Client Device on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.3 You shall not decompile, reverse engineer, disassemble or otherwise reduce any party of this Software to a humanly readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be provided by Kaspersky Lab on request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event Kaspersky Lab notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such steps to achieve interoperability provided that you only reverse engineer or decompile to the extent permitted by law.

1.1.4 You shall not permit any third party to copy (other than as expressly permitted herein), make error corrections to, or otherwise modify, adapt, or translate the Software nor create derivative works of the Software.

1.1.5 You shall not rent, lease or lend the Software to any other person, nor transfer or sub-license your license rights to any other person.

1.1.6 You shall not use this Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.

1.2 Server-Mode Use. You may use the Software on a Client Device or on or as a server (“Server”) within a multi-user or networked environment (“Server-Mode”) only if such use is permitted in the applicable price list or application packaging for the Software. A separate license is required for each Client Device or “seat” that may connect to the Server at any time, regardless of whether such licensed Client Devices or seats are concurrently connected to or actually accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g., “multiplexing” or “pooling” software or hardware) does not reduce the number of licenses required (i.e., the required number of licenses would equal the number of distinct inputs to the multiplexing or pooling software or hardware “front end”). If the number of Client Devices or seats that can connect to the Software exceeds the number of licenses you have obtained, then you must have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the license you have obtained. This license authorizes you to make or download such copies of the Documentation for each Client Device or seat that is licensed as are necessary for its lawful use, provided that each such copy contains all of the Documentation proprietary notices.

1.3 Volume Licenses. If the Software is licensed with volume license terms specified in the applicable application invoicing or packaging for the Software, you may make, use or install as many additional copies of the Software on the number of Client Devices as the volume license terms specify. You must have reasonable mechanisms in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each additional copy authorized by the volume license, provided that each such copy contains all of the Document’s proprietary notices.

2. Duration. This Agreement is effective for the period specified in the Key File (the unique file which is required to fully enable the Software, please see Help/ about Software or Software about, for Unix/Linux version of the Software see the notification about expiration date of the Key File) unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the conditions, limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must immediately destroy all copies of the Software and the Documentation. You may terminate this Agreement at any point by destroying all copies of the Software and the Documentation.

3. Support.

(i) Kaspersky Lab will provide you with the support services (“Support Services”) as defined below for a period of one year following:

(a) payment of its then current support charge, and;

(b) successful completion of the Support Services Subscription Form as provided to you with this Agreement or as available on the Kaspersky Lab website, which will require you to produce the Key Identification File which will have been provided to you by Kaspersky Lab with this Agreement. It shall be at the absolute discretion of Kaspersky Lab whether or not you have satisfied this condition for the provision of Support Services.

(ii) Support Services will terminate unless renewed annually by payment of the then-current annual support charge and by successful completion of the Support Services Subscription Form again.

(iii) By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy which is attached to this Agreement, and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.

(iv) “Support Services” means

(a) Daily updates of anti-virus database;

(b) Free software updates, including version upgrades;

(c) Extended technical support via E-mail and phone hotline provided by Vendor and/or Reseller;

(d) Virus detection and curing updates in 24-hours period.

4. Ownership Rights. The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all rights, titles and interest in and to the Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer any title to the intellectual property in the Software to you, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

5. Confidentiality. You agree that the Software and the Documentation, including the specific design and structure of individual programs and the Key Identification File constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide or otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab. You shall implement reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavors to maintain the security of the Key Identification File.

6. Limited Warranty

(i) Kaspersky Lab warrants that for [90] days from first download or installation the Software will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.

(ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free;

(iii) Kaspersky Lab does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus;

(iv) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item;

(v) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended or (c) use the Software other than as permitted under this Agreement;

(vi) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (v) have effect between the Kaspersky Lab and your or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

7. Limitation of Liability

(i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (i) the tort of deceit, (ii) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, (iii) any breach of the obligations implied by s.12 Sale of Goods Act 1979 or s.2 Supply of Goods and Services Act 1982 or (iv) any liability which cannot be excluded by law.

(ii) Subject to paragraph (i), the Supplier shall have no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):

(a) Loss of revenue;

(b) Loss of actual or anticipated profits (including for loss of profits on contracts);

(c) Loss of the use of money;

(d) Loss of anticipated savings;

(e) Loss of business;

(f) Loss of opportunity;

(g) Loss of goodwill;

(h) Loss of reputation;

(i) Loss of, damage to or corruption of data, or;

(j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraph (ii), (a) to (ii), (i).

(iii) Subject to paragraph (i), Kaspersky Lab's liability (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

8. The construction and interpretation of this Agreement shall be governed in accordance with the laws of England and Wales. The parties hereby submit to the jurisdiction of the courts of England and Wales save that Kaspersky Lab as claimant shall be entitled to initiate proceedings in any court of competent jurisdiction.

9. (i) This Agreement contains the entire understanding of the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab,

whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date. Save as provided in paragraphs (ii) - (iii), you shall not have any remedy in respect of an untrue statement made to you upon which you relied in entering into this Agreement ("Misrepresentation") and Kaspersky Lab shall not have any liability to the other than pursuant to the express terms of this Agreement.

(ii) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for any Misrepresentation made by it knowing that it was untrue.

(iii) The liability of Kaspersky Lab for Misrepresentation as a fundamental matter, including a matter fundamental to the maker's ability to perform its obligations under this Agreement, shall be subject to the limitation of liability set out in paragraph 7(iii).